Vysoká škola logistiky o.p.s.

Technologie Blockchain v logistických procesech

(Bakalářská práce)

Přerov 2022 Václav Hroch, DiS.

Vysoká škola logistiky o.p.s.

Zadání bakalářské práce

student	**Václav Hroch, DiS.**
studijní program	LOGISTIKA
specializace	Informatika pro logistiku

Vedoucí Katedry bakalářského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v bakalářském studijním programu určuje tuto bakalářskou práci:

Název tématu: **Technologie Blockchain v logistických procesech**

Cíl práce:

S využitím specializované, decentralizované, distribuované databáze blockchain založené na kryptograficky v čase chronologicky zaznamenaných transakcích popsat a navrhnout aplikační řešení technologie Blockchain v logistice.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Bakalářskou práci zpracujte v těchto bodech:

Úvod
1. Popis technologie Blockchain
2. Služby a aplikační možnosti technologie Blockchain v současné informační logistice
3. Návrh systémového využití platformy Blockchain v oblasti průmyslových transakcí
4. Vyhodnocení vlastního návrhu a možnosti aplikačního nasazaní

Závěr

Rozsah práce: 35 – 50 normostran textu

Seznam odborné literatury:

ELA Blockchain services [online]. Praha: Elektrotechnické asociace České republiky, 2019 [cit. 2021-10-30]. Dostupné z: https://www.elachain.cz

JAŠEK, Roman, Martin BURDÍK a Michal SEDLÁČEK. Blockchain v logistice. In: LOGISTIKA -EKONOMIKA - PRAX 2018: Mimoriadne číslo internetového portálu Logistický monitor - http://www.logistickymonitor.sk/images/prispevky/zborniklep-2018.pdf. Žilina: Logistický monitor, 2018, s. 61-68. ISSN 1336-5851.

LEE, David a Robert DENG, ed. Handbook of blockchain, digital finance, and inclusion. London: Academic Press, [2018]. ISBN 978-0-12-812282-2.

SOMMERVILLE, Ian. Softwarové inženýrství. Brno: Computer Press, 2013, 680 s. ISBN 9788025138267.

Vedoucí bakalářské práce: prof. Mgr. Roman Jašek, Ph.D., DBA

Datum zadání bakalářské práce: 31. 10. 2021
Datum odevzdání bakalářské práce: 6. 5. 2022

Přerov 31. 10. 2021

Ing. et Ing. Iveta Dočkalíková, Ph.D.
vedoucí katedry

prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená bakalářská je původní a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb., o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámen s tím, že se na mou bakalářskou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé bakalářské práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat předtím o této skutečnosti prorektora pro vzdělávání Vysoké školy logistiky o.p.s.

Prohlašuji, že jsem byl poučen o tom, že bakalářská práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované bakalářské práce v její tištěné i elektronické verzi. Souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze bakalářské práce, elektronická verze na odevzdaném optickém médiu a verze nahraná do informačního systému jsou totožné.

V Přerově, dne 06. 05. 2022 .....

podpis

Poděkování

Děkuji vedoucímu bakalářské práce, panu prof. Mgr. Romanovi Jaškovi, Ph.D., DBA, za pomoc, návrhy a cenné připomínky, které mě při zpracovávání vždy posunuly dále. Děkuji také své rodině a všem přátelům, kteří mě při vytváření této práce podpořili.

Anotace

Bakalářská práce je zaměřena na technologie, které dohromady vytváří blockchain. Popisuje vývoj blockchainu, princip fungování a způsoby využití v současné informační logistice. Blockchain je distribuovaná účetní kniha, která uchovává seznam všech transakcí. V rámci této práce je navržen koncept řešení využití technologie blockchain v oblasti průmyslových transakcí.

Klíčová slova

blockchain, distribuovaná účetní kniha, hash, logistika, proces

Annotation

The bachelor thesis focuses on the technologies that together make up the blockchain. It describes the development of blockchain, the principle of operation and how it can be used in contemporary information logistics. Blockchain is a distributed ledger that keeps a list of all transactions. This thesis proposes a solution concept for the use of blockchain technology in industrial transactions.

Keywords

blockchain, distributed ledger technology, hash, logistics, process

Obsah

Úvod

Ještě nedávno neměla většina lidí vůbec ponětí o pojmech blockchain, kryptoměny nebo bitcoin. Pojmy, za kterými se skrývá velmi zajímavý komplex různých technologií, se ale pomalu dostávají do povědomí veřejnosti. I přes to si asi málo lidí dokázalo představit jejich využití v průmyslových transakcích.

O popularizaci se zřejmě postaral dodnes neznámý, údajně japonský tvůrce jménem Satoshi Nakamoto, když na konci října roku 2008 nahrál na internet akademický článek pod názvem *Bitcoin: A Peer-to-Peer Electronic Cash System*. Publikaci, která popisovala první kryptoměnu bitcoin a zmiňovala pouze slovní spojení *chain of blocks*, v češtině tedy řetěz bloků.

Zřejmě až kvůli celosvětovému úspěchu bitcoinu se veřejnost více začala zajímat, jak celý systém decentralizované měny funguje. Postupně se začalo o bitcoin, respektive blockchain zajímat více odborníků napříč různými odvětvími. Vyšly různé studie, kde všude by systém decentralizované účetní databáze mohl nalézt uplatnění.

Blockchain nabízí vlastnosti, které lze využít i mimo finanční sektor. V dodavatelském řetězci se nabízí několik způsobů použití. Můžeme tuto technologii použít například pro sledování toku zboží a jeho původu. Do dodavatelského řetězce je mnohdy zapojeno více různých organizací, které vyžadují velké množství dokumentace, respektive byrokracie. Při výměně informací může docházet ke zpoždění, neúmyslným lidským chybám nebo cíleným podvodům. Použití blockchainové technologie však může tyto procesy zjednodušit a všechny informace uložit do jedné databáze, jejíž záznamy nelze zpětně měnit.

Cílem této bakalářské práce je popsat princip a možnosti využití technologie blockchain v logistických procesech. Pro zvolený problém navrhnout a popsat možnosti aplikačního nasazení v průmyslových transakcích včetně výsledného vyhodnocení.

1 Popis technologie Blockchain

Blockchain je technologie, o které se nejvíc mluví v souvislosti s bitcoinem. Je to dáno tím, že bitcoin je nejstarší kryptoměna a je nejvíce rozšířená. Poslední dobou se o blockchainu mluví díky vlastnostem, které má a kvůli možnému uplatnění mimo svět kryptoměn.

Jestliže klasické měny s nuceným oběhem (tzv. fiat měny) mají svůj vlastní finanční systém pro efektivní a bezpečné sdílení, tak jej mají i kryptoměny. První zmíněný systém je tvořen oficiálními bankami, finančními poradci, bankomaty, službami pro tisk bankovek atd. Naopak ten druhý je vybudován bez podílu třetích stran, tímto systémem je technologie blockchain. [1]

Pojmy blockchain, kryptoměna a bitcoin spolu souvisí, nicméně je potřeba je rozlišovat a chápat rozdílně, mnohdy totiž bývají označovány za totéž.

Jako příklad použiji jednoduchou analogii. Webové stránky jsou dobře známou internetovou aplikací pro sdílení informací Peer-to-Peer (P2P) (doslova přeloženo jako „rovný s rovným“). Internetové vyhledávače patří mezi nejběžnější způsob pro používání webových stránek, protože k nim usnadňují přístup. Nejznámějším a nejpoužívanějším internetovým vyhledávačem je Google od stejnojmenné společnosti Google.

Podobným způsobem spolu souvisejí blockchain, kryptoměna a bitcoin: blockchain je průlomová technologie pro ukládání a sdílení hodnot a informací online. Jak webových stránek, tak i blockchainů existuje mnoho různých druhů, které slouží různým účelům. Kryptoměny jsou zatím nejčastějším způsobem využití technologie blockchain. Bitcoin je jednou z mnoha existujících kryptoměn, ale je nejznámější a vůbec první kryptoměnou. [1]

1.1 Historie

V roce 2008 probíhala celosvětová finanční krize a svět hledal způsoby, jak zachránit současné peníze, bankovnictví a finance. V pátek 31. října 2008 se na internetu objevil akademický článek pojmenovaný „Bitcoin: A Peer-to-Peer Electronic Cash System“. Pod ním byl podepsán doposud neznámý pseudonymní tvůrce Satoshi Nakamoto. Základem byl tzv. whitepaper, tedy akademický článek.

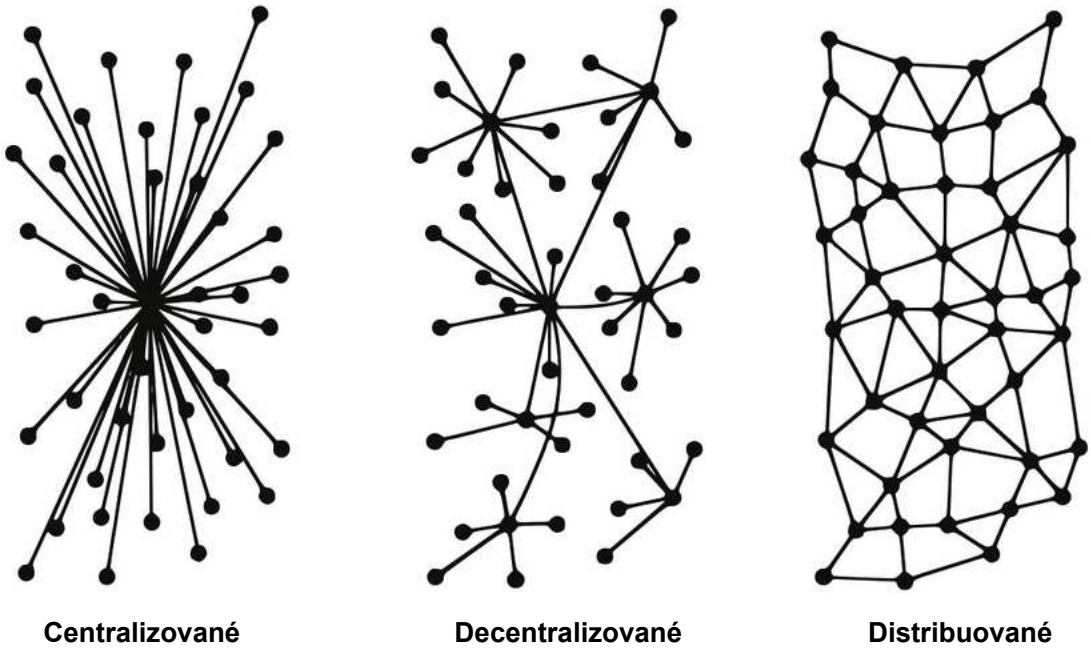
Zajímavostí je, že autor nezmínil ani jednou slovo „blockchain“, v článku se píše pouze o slovním spojení chain of blocks (řetěz bloků). Blockchain s ohledem na původní návrh

Satoshiho Nakamota není technologie sama o sobě, ale je výsledkem souhry několika technologií. [2]

Myšlenka, mít pro slovní výraz blockchain český ekvivalent, se objevila až v roce 2017 a je jím výraz *bločenka*. Pracovní návrhy byly také např. blokčejn, bloksíť, bloknet apod. Ovšem pojem bločenka se zatím moc nerozšířil. [3]

1.2 Architektura systémů

Rozlišujeme tři druhy architektur – centralizované, decentralizované a distribuované systémy.



Obr. 1.1: Druhy architektur systémů, Zdroj: [4], vlastní zpracování.

1.2.1 Centralizované

V centralizovaném systému jsou všichni uživatelé připojeni k jednomu centrálnímu vlastníkovi sítě, tzn. serveru. Server ukládá data, ke kterým mají ostatní uživatelé přístup a zároveň ukládá data o jeho uživatelích. Např. profily uživatelů, obsah jimi vytvořený atd. Centralizovaný systém se jednoduše nastavuje a dá se rychle vyvinout. Nevýhodou v centralizovaném systému je, že je závislý na centrálním uzlu (serveru), který připojuje všechny uživatele a zařízení. Jakmile dojde k poruše serveru, způsobí to kolaps celé sítě, protože v případě, že je server mimo provoz, není zde nic, co by jeho funkci nahradilo. Centrální

server data nejen ukládá, ale může k nim i přistupovat, což je další z bezpečnostních rizik spojených s centralizovanými systémy. [5]
Výhody centralizovaných systémů:

- rychlý vývoj a aktualizace,
- fyzické zabezpečení podle umístění,
- cenově dostupná údržba (mám pouze jeden server – nižší investice),
- praktické pro centrální kontrolu dat,
- jednoduché nasazení,
- snadné odpojení uzlu od systému.

Nevýhody:

- vyšší rizika pro bezpečnost a soukromí uživatelů,
- obtížnost údržby a tvorby záloh (pouze jeden server – nutnost vypnutí celé sítě),
- náchylnost k poruchám,
- delší odezva přístupu k datům pro vzdálenější uživatele. [5]

1.2.2 Decentralizované

Tyto systémy jsou dalšími, které narůstají na popularitě, především díky bitcoinu. Decentralizované systémy nemají centrální uzel. Místo něj mají hned několik centrálních uzlů, z nich každý má uloženou kopii prostředků, ke kterým mají uživatelé sítě přístup. V decentralizovaných systémech rozhoduje každý uzel sám za sebe. Konečné chování systému je souhrnem rozhodnutí jednotlivých uzlů. Decentralizovaný systém může být stejně náchylný k poruše jako centralizovaný. Ovšem při selhání jednoho nebo více centrálních uzlů, mají ostatní uživatelé stále přístup k datům, jestliže alespoň jeden z centrálních uzlů funguje. V tomto případě mohou majitelé systému opravit vadné uzly a vyřešit problémy, zatímco samotný systém běží dál jako obvykle. Výpadky uzlu mohou ovlivnit výkon a omezit přístup k některým datům. Avšak z hlediska celkové provozuschopnosti systému nabízí tato architektura velké zlepšení oproti centralizovanému systému. Přístupová doba k datům

je rychlejší, protože vlastníci mohou vytvářet uzly v různých oblastech nebo v oblastech s vyšší uživatelskou aktivitou. [5]
Výhody decentralizovaných systémů:

- lepší výkon – celá zátěž se vyrovná na všech uzlech,
- nezávislost jednotlivých uzlů,
- menší pravděpodobnost selhání oproti centralizovanému systému.

Nevýhody:

- vyšší náklady na údržbu,
- rizika pro bezpečnost a soukromí uživatelů,
- žádný regulační dohled.

Příkladem je bitcoin. Bitcoin je populárním využitím decentralizovaného systému. Bitcoinová síť nemá přímého vlastníka, žádný subjekt nebo organizaci. Síť je souhrnem všech uzlů, které spolu komuikují za účelem udržování množství bitcoinů, které má každý uživatel na účtu. [5]

1.2.3 Distribuované

Distribuovaný systém se skládá z několika uzlů (počítačů). Naopak u centralizovaného systému jsou všechny systémové komponenty spouštěny v jediném uzlu. Je to sestava nezávislých uzlů, která z uživatelského pohledu vypadá jako jeden spojitý systém. [6]

Distribuovaný systém kopíruje decentralizovaný, ale protože nemá jediného centrálního vlastníka, eliminuje centralizaci. Příkladem distribuovaného systému je samotný internet. Tento systém umožňuje uživatelům sdílet data. Mezi uživatele jsou rozděleny hardwarové a softwarové zdroje, což může v některých případech zlepšit výkonnost systému. Distribuovaný systém je chráněn před nezávislým selháním komponent, což může výrazně zlepšit jeho provozuschopnost. Vzhledem k různým omezením ostatních architektur byly vyvinuty distribuované systémy. Není tedy žádným překvapením, že technologie využívající distribuovaný systém, což je v našem případě blockchain, mění mnoho odvětví. [5]
Výhody:

- odolnost vůči poruchám,

- extrémně škálovatelný,
- podpora sdílení prostředků (výpočetního výkonu).

Nevýhody:

- vyšší náklady na údržbu,
- obtížnější nasazení. [5]

1.3 Definice blockchainu

Blockchain je posloupnost (sekvence, řetěz) bloků, které obsahují kompletní přehled provedených transakcí podobně jako běžná veřejná účetní kniha. [7]

Podobně jako v běžné účetní knize je zaznamenán veškerý pohyb, např. převody peněz, pohyb materiálu, zásob atd., tak úplně stejně to funguje na blockchainu. Jedná se o specifickou databázi s online záznamy. Od centralizované se liší tím, že nemá pouze jednoho, ale hned několik správců (uzlů). Je v síti velkého množství počítačů, které na této síti spolupracují, po celém světě.

Uzly těží kryptoměnu tím, že vytvářejí (uzavírají) bloky pro transakce požadované v síti. Těžaři (z angl. miners) jsou jako bankovní pokladníci nové doby, kteří formulují transakce a za své úsilí dostávají (neboli těží) poplatek. [8]

Záznamy jednotlivých transakcí se do této účetní knihy zapisují na základě vzájemné shody. Aby ke shodě mohlo dojít, jsou těžaři dle nastavených pravidel (podrobněji kapitola 1.8) finančně motivovaní k ověřování transakcí. Za ověření transakce získají odměnu v kryptoměně v určité výši, kterou dále mohou směnit prostřednictvím kryptosměnárny za klasickou fiat měnu. Takto lze v podstatě do nekonečna ukládat další a další transakce, bez nutnosti centrálního dohledu. [9]

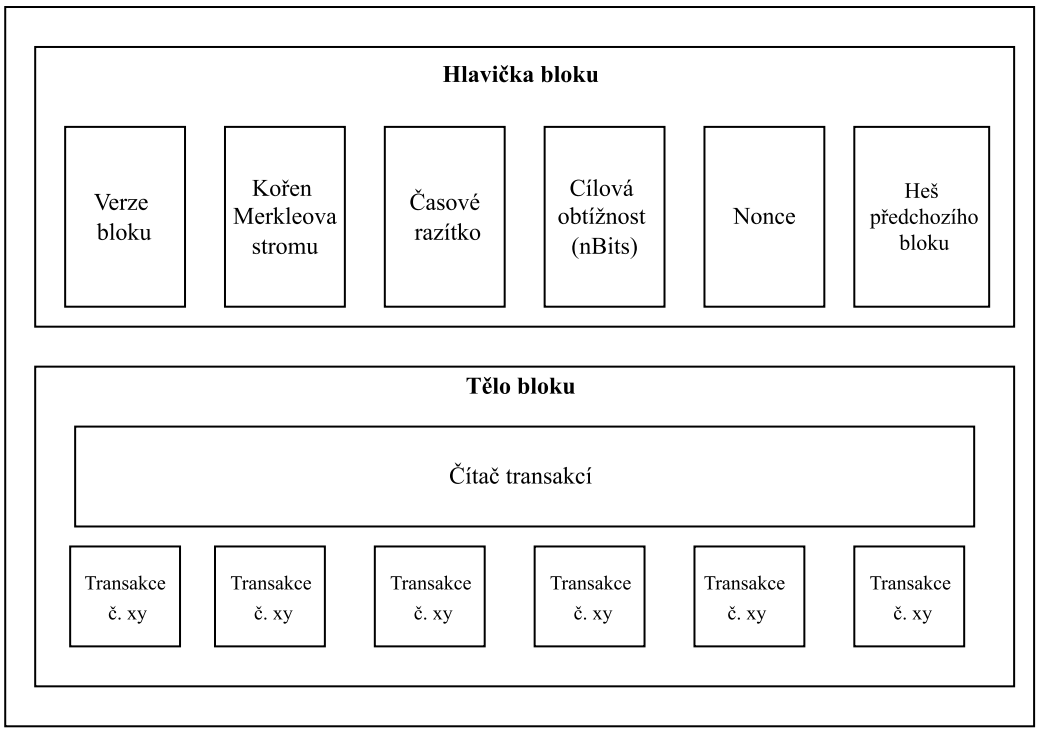
Blockchain je distribuovaná decentralizovaná databáze, ve které se uchovává neustále se rozšiřující řetězec chronologicky po sobě jdoucích záznamů (bloků). Tento řetězec je propojen zabezpečenými P2P uzly. Data, která byla zanesena do blockchainu, tam tedy jsou uložena trvale a jsou až na pár výjimek (viz kapitola 1.4) veřejně přístupná. [9]

Analogicky si lze blockchain představit na domě postaveném z cihel. Neexistuje způsob, jak odstranit cihlu z prostřední řady domu aniž by se nenarušila celá jeho struktura.

1.3.1 Blok

Blok (z angl. block) je místo, kam se ukládají data o provedených transakcích. Tyto bloky jsou uspořádány v lineární sekvenci, která tvoří nekonečný řetězec bloků = blockchain. Záznamy vedou až k prvnímu bloku, který se označuje jako genesis blok (blok nula). Tento blok jako jediný nemá rodičovský blok, protože je první. Počet potvrzených bloků od prvního bloku je označována jako **výška bloku**. [10]

Blok je složen z hlavičky bloku a jeho těla. Tělo bloku se skládá z čítače transakcí (číslo, které představuje počet transakcí uložených v bloku) a seznamu všech provedených transakcí v rámci bloku. Maximální možný počet transakcí, které může každý blok obsahovat, je závislý na velikosti bloku a velikosti každé transakce. [7]



Obr. 1.2: Stavba bloku, Zdroj: [7], vlastní zpracování.

Na obrázku 1.2 je vidět co téměř každá hlavička bloku obsahuje, zleva:

- verzi bloku,
- kořen Merkleova stromu – hodnota heše všech transakcí uvnitř bloku,
- časové razítko – udává čas vytvoření bloku,

- cílová obtížnost (nBits) – použitá obtížnost při tvorbě bloku,
- nonce (number only used once) – libovolné celé číslo, které obvykle začíná nulou a zvyšuje se s každou kalkulací heše,
- heš předchozího bloku (rodičovského bloku).

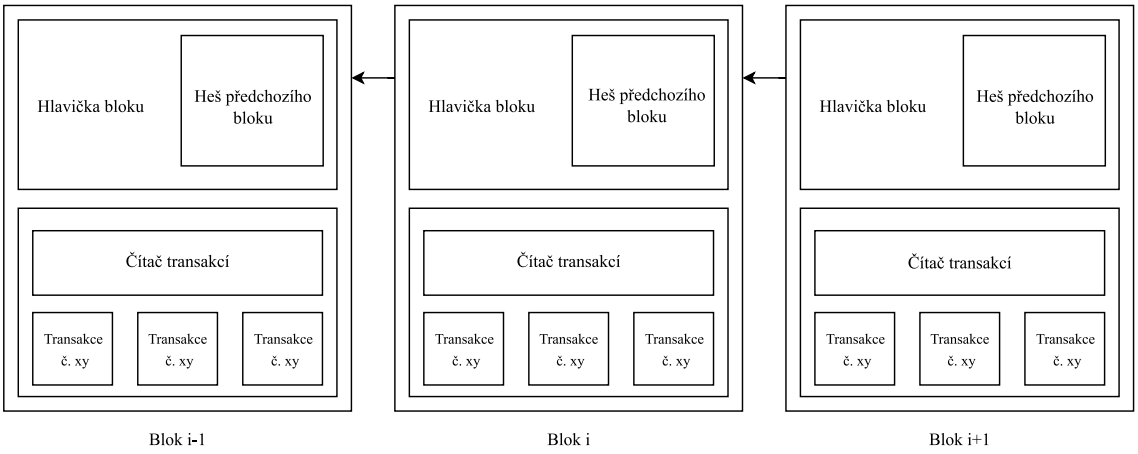
Blockchain využívá asymetrické kryptografie k ověřování pravosti transakcí podobně jako digitální podpis. [7]

Unikát (nonce) jednorázové unikátní číslo, pomocí kterého se individualizuje vykonání kryptografického algoritmu. Pro představu šifrování stejné zprávy stejným klíčem nám unikát zajistí vždy jiný výsledek šifrování. Důsledkem individualizace algoritmu je skutečnost, že útočník nemůže jednoduše provést řadu útoků a to mu značně komplikuje provádění kryptoanalýzy.

Unikáty dělíme na odhadnutelné a neodhadnutelné.

U odhadnutelných unikátů může útočník lépe předpokládat jejich konkrétní hodnoty. Většinou se jedná o aktuální časový údaj (časové razítko), čítač transakcí či pořadové číslo zprávy (sequence number). Hodnoty u neodhadnutelných unikátů se nedají předpokládat, protože jde o náhodně zvolená čísla. Rozsah těchto hodnot je nutné volit tak, aby se po dobu platnosti daného klíče hodnoty těchto unikátů neopakovaly nebo se pravděpodobnost užití stejné hodnoty blížila nule. [11]

Na obrázku 1.3 je vidět sekvence jednotlivých bloků. Každý blok (kromě genesis bloku) má svůj rodičovský blok, který je vázán pomocí kryptografického heše. Heš, který se připojuje na konec blockchainu se tak nepočítá jen z posledního připojeného bloku. Do jeho výpočtu se zahrnují i heše předchozího bloku. Při pokusu změnit cokoliv v některém z bloků blockchainu, změní všechny následující heše včetně posledního. Potom lze jednoduchým porovnáním s ostatními kopiemi blockchainu snadno zjistit, že se jedná o podvrh.



Obr. 1.3: Sekvence bloků, Zdroj: [7], vlastní zpracování.

1.3.2 Princip transakce

Na první místě jsou uživatelé, kteří chtějí využít mechaniku blockchainu k uskutečnění transakce. Vzhledem k tomu, že není k dispozici centrální autorita, která by transakci provedla a tím ji ověřila, nastupují těžaři. Těžaři ověřují příchozí transakční bloky – dávky požadovaných transakcí, které čekají v mempoolu (paměťovém fondu, ve fázi mezi požadavkem a přidáním do blockchainu) na potvrzení. Správné provedení tohoto úkonu znamená odměnu pro těžaře, což je pobídka, která udržuje systém v chodu. Na posledním místě jsou uzly. Uzly udržují celý systém v bezpečí tím, že ověřují bloky transakcí odeslané těžaři před jejich přidáním do blockchainu. Kontrolují příchozí informace s transakční historií blockchainu, aby se ujistily, že vše souhlasí. Uzly sítě, jež jsou roztroušené po celé planetě, pak společně dosáhnou konsenzu (shody). To znamená, že nové transakce jsou platné, a teprve poté jsou přidány do blockchainu. [12]

Transakce se mohou týkat kryptoměn, smluv, záznamů nebo jiných informací. Proces průběhu transakce lze rozdělit do šesti kroků:

1. požadavek na provedení transakce,
2. transakce je vyslána do všech P2P uzlů v blockchainu,
3. transakci ověří těžaři podle stanovených pravidel,
4. ověřená transakce je uložena do bloku a zapečetěna hešem,
5. nový blok je přidán do blockchainu po ověření heše,
6. transakce je dokončena.

Všechny transakce jsou zveřejněny v paměťovém fondu, kde jsou považovány za „čekající“. V rámci transakce platí uživatelé transakční poplatky, které kompenzují výpočetní energii potřebnou ke zpracování a ověření transakcí v blockchainu. Po dokončení transakce se stává součástí blockchainu a nelze ji nijak změnit. [12]

1.3.3 Klíčové výhody blockchainu

Decentralizace

Výhodou je nezávislost na centrálních autoritách a zprostředkovatelích transakcí, tzn. absence třetí strany. Výjimkou jsou soukromé blockchainy, které však čerpají výhod decentralizace, přestože jsou spravovány či řízeny centrálně. Konzistenci dat hlídají konsenzuální algoritmy. [7]

Neměnnost

Je téměř nemožné smazat nebo vrátit zpět transakce, jakmile jsou jednou zařazeny do blockchainu. [7]

Anonymita

Každý uživatel může vystupovat pod vygenerovanou adresou, která neprozrazuje jeho skutečnou identitu. [7]

Ověřitelnost

Všechny transakce jsou zaznamenány v blockchainu. Díky kompletní historii je možné transakce zpětně ověřit a sledovat. [7]

1.4 Varianty blockchainu

Postupem času se objevilo více variant blockchainu. Nejčastěji se dělí na veřejný a soukromý blockchain, dále potom na blockchainy pro obchodní společnosti (konsorcia) a hybridní blockchainy.

1.4.1 Veřejný

Veřejné blockchainy jsou přístupné bez oprávnění, umožňují připojení komukoli a jsou zcela decentralizované. Umožňují všem uzlům mít stejná práva k přístupu do blockchai-

nu, vytváření nových bloků dat a ověřování bloků dat. Používají se především k výměně a pro těžbu kryptoměn. Veřejné blockchainy mají obvykle delší dobu ověřování nových dat oproti soukromým blockchainům a soukromé jsou zranitelnější vůči podvodům. K odstranění těchto nevýhod byly vyvinuty konsorciální a hybridní blockchainy. Populární veřejné blockchainy jsou např. Bitcoin, Ethereum a Litecoin. [8]

1.4.2 Soukromý

Soukromé blockchainy je možné označit též jako spravované blockchainy, jsou přístupné pouze s povolením, které kontroluje jedna organizace. Centrální autorita určuje, kdo může být uzlem. Centrální autorita také nemusí každému uzlu nutně udělovat stejná práva k výkonu funkcí. Soukromé blockchainy jsou decentralizované pouze částečně, protože přístup veřejnosti je omezen. Příkladem soukromých blockchainů je síť pro výměnu virtuálních měn mezi podniky Ripple a Hyperledger, zastřešující projekt open-source blockchainových aplikací. [8]

1.4.3 Konsorciální

Konsorciální blockchainy spravuje skupina organizací (konsorcium), nikoli jeden subjekt, jako je tomu v případě soukromých. Mají proto větší decentralizaci, což vede k vyšší úrovni bezpečnosti. Vytváření konsorcií však může být náročné, protože vyžaduje spolupráci více organizací, což představuje logistické problémy i potenciální antimonopolní riziko. Dále někteří z členů dodavatelského řetězce nemusí mít potřebnou technologii ani infrastrukturu pro implementaci blockchainových nástrojů. [8]

1.4.4 Hybridní

Hybridní blockchainy jsou řízeny jednou organizací, ale s určitou úrovní dohledu zajištěného veřejným blockchainem, který je nutný k provádění určitých validací transakcí. [8]

1.5 Vývoj blockchainu

Podobně jako se postupně historicky vyvíjí průmysl, můžeme analogicky popsat vývoj blockchainu.

Blockchain 1.0

Myšlenku pro tvorbu peněz prostřednictvím řešení výpočetních hádanek poprvé představil Hal Finney v roce 2005. Vytvořil první koncept pro kryptoměny (implementaci distribuované účetní knihy). Tato účetní kniha umožňuje provádět finanční transakce založené na blockchainu. Bitcoin je neznámějším příkladem v tomto odvětví. Používá se jako hotovost na internetu a bývá označován za spouštěče tzv. Internetu peněz. [13]

První generace blockchainu měla za úkol vylepšit tradiční měnový systém. v této generaci byl představen bitcoin a další kryptoměny, využívající konsenzuální algoritmus Proof of Work. Kryptoměny založené na blockchainu zlepšily zkušenosti s transakcemi a vývojáři si uvědomili, že tato technologie má velký potenciál i mimo kryptoměny. To bylo důvodem pro vznik druhé generace. [14]

Blockchain 2.0

Hlavní problémy, které se objevily u Bitcoinové sítě, plýtvání těžbou a nedostatečná škálovatelnost sítě. K vyřešení těchto problémů druhá generace rozšiřuje koncept bitcoinu nad rámec měny. Novými klíčovými koncepty jsou chytré kontrakty (z angl. Smart contracts). Jedná se o malé počítačové programy, které běží v blockchainu. Automaticky se pouští a ověřují podmínky, které byly definovány dříve, jako je usnadnění, ověření nebo vynucení. Velkou výhodou této technologie, kterou blockchain nabízí je, že znemožňuje manipulaci nebo hackování chytrých kontraktů. Nejvýznamnějším příkladem je Ethereum Blockchain, který poskytuje platformu, kde může komunita vývojářů vytvářet distribuované aplikace pro síť blockchain. [13]

Blockchain 3.0

Třetí generace blockchainu se soustředí na efektivnější řešení založená na blockchainu. Vývojáři blockchainových aplikací se zaměřili na využití různých konsenzuálních algoritmů, než jenom algoritmu Proof of Work (PoW). [14]

Především kvůli tomu, že nejvíce používaný konsenzuální algoritmus PoW, je velmi náročný na spotřebu elektrické energie.

Blockchain 4.0

Podniky se předhánějí v implementacích blockchainu a tím z něj činí klíčový prvek svých technologických řešení. Blockchain 4.0 přináší přístupy a řešení pro průmyslová od-

větví. Průmysl 4.0 se zaměřuje na automatizaci a plánování podnikových zdrojů. Blockchain pomáhá této průmyslové revoluci tím, že poskytuje stále větší míru ochrany soukromí a bezpečnosti. [14]

1.6 Kryptografie

Kryptografie vznikla důsledkem přirozené potřeby zpřístupnit písemné záznamy jen oprávněným osobám, tzn. že vznik kryptografie byl podmíněn vznikem písma. Nejstarším známým důkazem o využití kryptografie je hliněná destička z Mezopotámie s šifrovaným popisem technologie výroby glazované keramiky. Tato destička je datována do období 1500 let př. n. l. a dokazuje tak, že kryptografické techniky lidstvo používalo již před zhruba 3500 lety. [11]

Nejvýznamnějším mezníkem vývoje kryptografie jsou sedmdesátá léta minulého století. V roce 1974 byl publikován koncept symetrických autentizačních kryptosystémů, kdy se zjistilo, že kromě utajování zpráv, je možné zajistit i jejich autentičnost. V roce 1978 byl zveřejněn první asymetrický utajovací kryptosystém RSA (iniciály autorů Rivest, Shamir, Adleman) spolu s konceptem digitálního podpisu. [11]

V kryptografii se k základním matematickým operacím využívají logické operace, což jsou operace s bity, tzn. operace s proměnnými, které mohou nabývat dvou hodnot, jedničky a nuly.

1.6.1 Kryptografický systém

Algoritmus je výpočetní postup pro řešení určité úlohy. Kryptografickým protokolem rozumíme algoritmus, na jehož provádění se podílí více stran (např. původce i adresát). Potom lze kryptografickému systému (kryptosystému) rozumět jako algoritmu určenému k zajištění důvěrnosti a / nebo autentičnosti zpráv.
V praxi se používají následující typy kryptosystémů:

- utajovací kryptosystémy – zajišťují jen důvěrnost zpráv,
- autentizační kryptosystémy – zajišťují jen autentičnost zpráv,
- hybridní kryptosystémy – zajištují důvěrnost i autentičnost zpráv.

1.6.2 Důvěrnost, autorizace, autenticita

V souvislosti s kryptosystémy se lze setkat s různými pojmy, které se však často pletou.

Zajištění důvěrnosti (z angl. privacy), jde o zajištění toho, aby se s daným obsahem (např. obsahem dokumentu) nemohl seznámit nikdo jiný. Předmětný obsah se samozřejmě může dostat do rukou jiné osoby, avšak dané osobě není umožněno seznámit se s důvěrným obsahem. V praxi je důvěrnost zajištěna použitím vhodného zašifrování příslušného obsahu. [15]

Dalším základním pojmem je **autorizace** (z angl. authorization). V rámci autorizace jde o práva pro určité úkony či aktivity. (např. právo provést změnu v určitém dokumentu, smazat nějaký soubor atd.) V užším smyslu se pak autorizací rozumí udělení práva jen pro určitý úkon. V širším smyslu jde o celou správu oprávnění, která mají konkrétní subjekty a to včetně přidělování a odebírání těchto práv. [15]

Autenticita neboli pravost dokumentu značí, že se stále jedná o ten stejný dokument a nebyl nikým vyměněn za jiný. Např. autenticitu porušíme velmi snadno tím, že v dokumentu něco změníme, nebo jej zaměníme nějakým jiným dokumentem. [15]

1.6.3 Kryptografické proměnné

Sem patří klíče, z matematického hlediska to jsou číselné parametry, které v rámci určité množiny všech šifrovacích nebo pečetících funkcí definují konkrétní použitou funkci. Klíče se většinou dělí podle typu a účelu daného kryptosystému, nejčastěji:

- symetrický:
  - utajovací (šifrovací a dešifrovací klíč),
  - autentizační (pečetící klíč a ověřovací klíč),
- asymetrický:
  - utajovací (veřejný šifrovací klíč, soukromý dešifrovací klíč),
  - podepisovací (soukromý podepisovací klíč, veřejný ověřovací klíč).

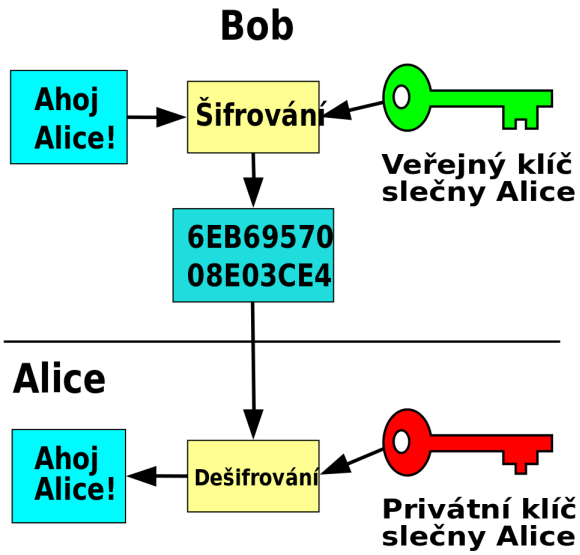
V případě symetrických kryptosystémů jsou klíče všech zúčastněných stran tajné. Pro asymetrické kryptosystémy se v tajnosti udržuje pouze soukromý klíč a druhý z klíčů zůstává veřejný. V utajovacím kryptosystému je soukromým klíčem klíč dešifrovací, u podepisovacích kryptosystémů je soukromým klíčem podepisovací klíč. [11]

1.7 Asymetrická kryptografie

Jak již bylo zmíněno dříve, blockchain se skládá z několika různých technologií. Nejčastějším využitím je ukládání transakcí. Jestliže chceme ukládat správná data o provedených transakcích musíme nějakým způsobem ověřit toho, kdo transakci provedl. K tomu se v blockchainu využívá asymetrické kryptografie.

Bloky jsou do existujícího blockchainu přidány až po jejich ověření. Toho lze dosáhnout různými způsoby. Asymetrická kryptografie (neboli šifrování veřejným klíčem) využívá pro šifrování a dešifrování různé klíče. Máme pár klíčů, veřejný (angl. public) klíč a soukromý (angl. private) klíč. Přičemž veřejný klíč je zveřejněn a odpovídající soukromý klíč musí zůstat v tajnosti. Data zašifrovaná veřejným klíčem lze dešifrovat pouze pomocí odpovídajícího soukromého klíče. Přestože soukromý a veřejný klíč spolu matematicky souvisí, není možné vypočítat soukromý klíč z veřejného klíče. [16]

Na obrázku 1.4 vidíme, jak v praxi probíhá šifrování a dešifrování zprávy, kterou Bob chce poslat Alici.



Obr. 1.4: Asymetrická kryptografie, Zdroj: [17].

1.7.1 Jednosměrné funkce

Jednosměrné funkce v kryptografii dělíme na:

- funkce s pevnou délkou výstupu,
- funkce s volitelnou délkou výstupu.

Jednosměrná funkce f, je funkce, pro jejíž libovolný vzor x, můžeme snadno vypočítat obraz y, ovšem pro daný obraz y je prakticky nemožné vypočítat jeho vzor.

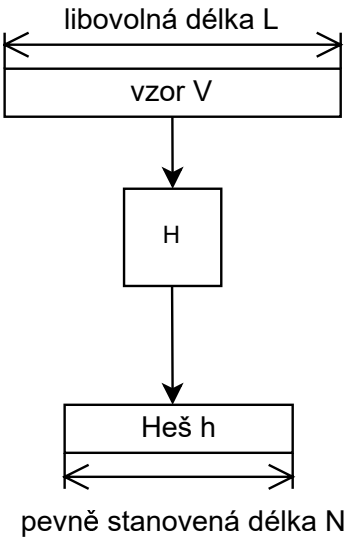
Jednosměrné funkce s pevnou délkou výstupu přiřazují vzoru o libovolné bitové délce určitý obraz s pevně stanovenou délkou. Tato funkce se obvykle nazývá hešovací funkce (z angl. hash function). Nejčastěji se využívá k tomu, abychom zprávě Z přiřadili relativně krátký bitový řetězec s pevně stanovenou délkou, který pak slouží jako reprezentant (otisk) Z. U funkce s volitelnou délkou výstupu je bitová délka obrazu volitelná. Délka výstupu záleží na použití určitého druhu funkce, buď může být kratší než vstup (kompresní), stejná (ekvivalentní), nebo delší (expanzní funkce). V kryptografii se nejvíce používají expanzní jednosměrné funkce. Třida těchto funkcí se obvykle používá k odvozování klíčů a ke generování bitových posloupností.[11]

1.7.2 Hešovací funkce

Heš (hash) je matematická funkce, která transformuje vstup libovolné délky na výstup s pevně danou délkou, která se liší podle volby typu hešovací funkce. Tento konsenzuální algoritmus je soubor pravidel, který reguluje fungování blockchainové sítě. Vyjma kryptoměn je nejrozšířenější aplikací hešovacích funkcí ukládání hesel. Hlavním účelem těchto funkcí, viz obrázek 1.5, je vytvářet otisky zpráv o konstantní délce, tzv. heše.

Vzorem pro hešovací funkci H je binární posloupnost v (obvykle nějaká zpráva) o libovolné délce L bitů a obrazem funkce je binární posloupnost h (tzv. heš) s pevnou délkou N (typicky 128 až 512 bitů). [11, str. 37]

Vzhledem k délkám vzorů L a hešů N platí, že počet prvků množiny vzorů je několikanásobně větší než počet prvků množiny hešů. Důsledkem toho je fakt, že každý heš reprezentuje více vzorů. Tomuto jevu říkáme kolize vzorů. [11]



Obr. 1.5: Účel hešovací funkce, Zdroj: [11], zpracování vlastní

.

Požadavky na hešovací funkce:

- odolnost vůči získání vzoru (preimage resistance),
- odolnost vůči modifikaci vzoru (2nd-preimage resistance),
- odolnost vůči kolizím (collision resistance).[11]

Každá i sebemenší změna v datech způsobí změnu heše, viz tabulka 1.6, která ukazuje rozdíl výstupních hešů, které jsou způsobeny pouhou změnou velikosti počátečního písmene ve slově *blok*.

Tab. 1.6: Vstupy a jejich výstupní heše

Vstup	**Výstupní heš (funkce SHA-256)**
Blok	d37acb9022fbf0a958f693e6c524f542f73aa1b7cca5cdb219b122feffddd127
blok	32376d85db3733ed7e2e4b1cc1cf313d6faeec3f6de7241b9387e7f0fe4c35c9

Zdroj: Vlastní zpracování

Hešovací funkce SHA-256

Tato hešovací funkce má délku heše 256 bitů a patří do rodiny funkcí Secure Hash Algorithm (SHA-2). Hešovací funkce SHA-256 byla standardizována naposledy v roce 2012 a patří mezi nejpoužívanější. [11]

1.8 Konsenzuální algoritmy

Konsenzuální algoritmus (mechanismus nebo protokol) je základním stavebním pilířem decentralizovaného systému. Konsenzem rozumíme obecné dosažení shody. Např. pokud se rozhodneme jít do kina se skupinou lidí a dojde k vzájemné shodě na vybraném filmu, dojde k tzv. konsenzu. V blockchainu dojde ke konsenzu v případě, že se alespoň 51 % uzlů v síti shodne na dalším globálním stavu sítě, jako jsou např. zůstatky na účtech a pořadí transakcí. V kryptoekonomickém systému pomáhá konsenzuální algoritmus předcházet určitým druhům ekonomických útoků. Teoreticky může útočník shodu ohrozit tím, že ovládne 51 % sítě, nicméně konsenzuální algoritmy jsou navrženy tak, aby tento útok znemožnily. [18]

Konsenzuální algoritmy zajišťují zachování integrity dat ve všech kopiích sdílené účetní knihy. Aby bylo případně možné jednoznačně určit, které kopie jsou pravé, protože se mohou vyskytnout nesrovnalosti, např. vlivem chyb, zpoždění nebo podvodu. Pro kontrolu shody se v Bitcoinové síti používá protokol Proof of Work. [19]

1.8.1 Proof of Work

Myšlenku Proof of Work (PoW) v překladu „důkaz prací“, poprvé zvěřejnili Cynthia Dwork a Moni Naor v roce 1993, kteří předpokládali uplatnění v boji proti hackerským útokům a spamu. Později metodiku použil Satoshi Nakamoto v bílé knize o bitcoinu v roce 2008. PoW je konsenzuální algoritmus, který se používá u většiny kryptoměn, které jsou v oběhu. Principem PoW je, že je obtížné najít řešení, ale je snadné jej ověřit. Důkaz prací spočívá v tom, že těžaři poskytují výpočetní výkon a hledají řešení složité matematické hádanky, aby mohl být nový blok připojen do stávajícího blockchainu. Jakmile těžař složitou hádanku vyřeší (najde správné řešení), uzel ji rozešle do celé sítě. Za vyřešení obdrží odměnu za vynaloženou práci (odtud název důkaz prací) v kryptoměně. [20]

V době psaní této práce je odměna (výplata) za uzavření (vytěžení) jednoho bloku v Bitcoinové síti 6,25 bitcoinu. Množství bitcoinů, které je možné získat za těžbu se každé čtyři roky sníží na polovinu (tak je totiž Bitcoinová síť navržena). Poslední půlení bitcoinu proběhlo 11. května 2020, další půlení tedy proběhne v roce 2024.
Jak je vidět, PoW je dán konkurencí a výpočetním výkonem. Představte si matematickou olympiádu, kde je soutěžícím (těžařům) zadán dosud nevyřešený důkaz (blok). Kdo tento důkaz vyřeší jako první, získá cenu (odměnu za blok) a vyřešený důkaz je poté zveřejněn

na internetu, aby ho všichni viděli (blok je přidán do blockchainu).

Především se PoW využívá v prostředí kryptoměn, nicméně kromě toho že je vysoce nákladný, neumožňuje vyšší frekvenci přidávání bloků do blockchainu, protože výpočet matematické úlohy trvá dlouho. Proto vznikla řada dalších konsenzuálních algoritmů, které se pro jiné typy blockchainů hodí více.

1.8.2 Proof of Stake

Další je Proof of Stake (PoS), v překladu „důkaz sázkou“. Nikdo nic netěží, ale pouze ověřuje, proto se místo pojmu těžař, používá pojem **validátor**. Algoritmus spočívá v tom, že čím více kryptoměny validátor investuje (vsadí) do systému, tím méně ho bude chtít zneužít. Na rozdíl od PoW, který funguje na principu těžby, je proto PoS energeticky úspornější a efektivnější. Validátor bloku je určen výší investice (sázky) nikoliv podle výpočetního výkonu jako u PoW. Validátor vsadí (uzamkne) určité množství kryptoměny (liší se podle konkrétní sítě) a tím zaručí správnost transakce (dá možnost ověřit bloky). Validátoři jsou vybíráni náhodným procesem. V případě, že se validátor pokusí systém podvést (ověří špatný blok), vsazená část kryptoměny mu je zabavena jako trest za nepoctivou práci. Výše částky, o kterou přijde, závisí na konkrétní síti. Implementace PoS algoritmu je v každém druhu blockchainu trochu odlišná. [7]

1.8.3 Proof of Capacity

V algoritmu Proof of Capacity (PoC) validátoři místo do drahého hardwaru, investují svůj prostor na pevném disku ve svém počítači. Čím více místa na pevném disku mají, tím větší je jejich šance, že budou vybráni pro ověření (těžbu) dalšího bloku a získají odměnu za blok. [21]

1.8.4 Proof of Elapsed Time

Proof of Elapsed Time (PoET) je jedním z nejspravedlivějších konsenzuálních algoritmů. Je hodně používán v soukromých blockchainech. V tomto algoritmu má každý validátor v síti stejnou šanci vytvořit svůj vlastní blok. Všechny uzly čekají náhodně dlouhou dobu. První, komu doba vyprší, přidá nový blok do chainu a informuje ostatní uzly. V algoritmu jsou další kontroly, které hlídají, aby uzel čekal přidělenou dobu, a nezačal zveřejňovat dříve či se nesnažil zneužít systém. PoET nepodporuje decentralizaci a otevřenost jako PoW, protože vyžaduje vydání certifikátu každému, kdo se chce k síti připojit. [21]

2 Služby a aplikační možnosti technologie Blockchain v současné informační logistice

Tato kapitola se zabývá příklady současného využití technologie blockchain. Tato technologie je ve srovnání s tradičními postupy výměny informací poměrně nová, nicméně velké korporace se snaží čím dál více své procesy digitalizovat a tím je samozřejmě zjednodušit. S využitím blockchainu můžeme zajistit transparentnost, bezpečnost, rychlost, zpětnou dohledatelnost, to vše efektivně v rámci jedné sítě, což je v oblasti informační logistiky žádoucí.

Množství příkladů a studií využití blockchainových technologií se neustále rozšiřuje, proto zde uvádím jenom některé z nich. Ve spojení blockchain a dodavatelský řetězec se objevuje zkratka IBM, je to název americké mezinárodní technologické společnosti International Business Machines Corporation (IBM), která je průkopníkem využití této technologie a také vývojářem vlastní blockchainové aplikace.

Další možností, jak využít blockchain, je koncept chytrých kontraktů (Smart contracts).

2.1 Definice informační logistiky

Logistika je obecně zaměřena především na efektivitu řízení toku materiálu. V širším slova smyslu se jedná o řízení a kontrolu všech zdrojů, a to včetně těch informačních. Informační logistiku lze definovat v podobném duchu, jako je metodika řízení 5 S, která se používá hlavně ve štíhlé výrobě. Správná informace musí být na správném místě ve správný čas. Dosažení tohoto cíle však není tak snadné i přes vyspělost informačních technologií, vzhledem k tomu, že do toho pořád vstupuje lidský faktor. Postupnou eliminací aktivit, které závisí na lidském faktoru můžeme dosáhnout úspěchu. Například ve firemní komunikaci se velká část informací vyloženě duplikuje nebo se naopak zbytečně ztrácí ve složitých emailových komunikacích, čemuž by měla správně nastavená informační logistika předcházet. [22]

2.2 Platforma Hyperledger Fabric

Hyperledger Fabric je open-source (software s otevřeným zdrojovým kódem) platforma navržená pro podnikové použití v rámci soukromého blockchainu. Spravuje jej ne-

zisková organizace Linux Foundation, která byla založena za účelem propagace platformy Linux. Hyperledger Fabric disponuje vysoce modulární a konfigurovatelnou architekturou, která zahrnuje inovace, všestrannost a optimalizaci pro širokou škálu použití v průmyslových podnicích, včetně bankovnictví, financí, pojištění, zdravotnictví, lidských zdrojů, dodavatelského řetězce a dokonce i poskytování digitální hudby.

Hyperledger Fabric je první platformou, která podporuje chytré kontrakty (podrobněji kapitola 2.5) napsané v univerzálních programovacích jazycích (Java, Go a Node.js) a nikoliv v omezených specifických jazycích. To znamená, že většina podniků již má potřebné dovednosti pro vývoj chytrých kontraktů a není tak potřeba žádné další školení. Jednou z nejdůležitějších odlišností platformy je podpora modulárních konsenzuálních algoritmů, které umožňují efektivnější přizpůsobení platformy konkrétním případům použití. Hyperledger Fabric může využívat konsenzuální algoritmy, které nevyžadují podporu kryptoměn. Vyhnutí se kryptoměně snižuje některá významná rizika útoku a absence kryptografických těžebních operací znamená, že platformu lze nasadit s přibližně stejnými provozními náklady jako jakýkoliv jiný distribuovaný systém. Kombinace těchto odlišujících konstrukčních prvků činí z Hyperledger Fabric jednu z nejvýkonnějších platforem, které jsou dnes k dispozici, a to jak z hlediska zpracování transakcí, tak z hlediska odezvy potvrzování transakcí. [23]

Mnoho projektů funguje na platformě Hyperledger Fabric, možná právě proto, že je open source, tedy snižuje cenu implementace narozdíl od toho, kdybychom se rozhodli vybudovat si vlastní blockchain od A do Z.

2.2.1 Modularita

Hyperledger Fabric je platforma navržená, jako modulární, aby bylo možné co nejvíce přizpůsobit konfiguraci pro specifické podnikové použití. Ať už jde o modularitu konsenzuálních algoritmů, protokolů správy identity, protokolů pro správu klíčů nebo kryptografických knihoven. Chytré kontrakty běží odděleně v kontejnerovém (virtualizovaném) prostředí, kvůli izolaci.

V průmyslu neexistuje jeden blockchain, který by používali všichni. Hyperledger Fabric lze nakonfigurovat mnoha způsoby, aby splňoval specifické požadavky na řešení pro různé případy použití. [23]

2.3 Použití v dopravě

2.3.1 Platforma TradeLens

V roce 2018 na akci THINK'18 v San Franciscu společnosti Maersk (jeden z největších provozovatelů kontejnerové dopravy) a IBM (americká mezinárodní technologická společnost) oznámily, že spojí své síly a vytvoří digitální platformu založenou na blockchainu speciálně pro lodní dopravu. Platformu TradeLens, řešení, které změní celý dodavatelský řetězec včetně logistiky. Projekt TradeLens již přitáhl pozornost více než 170 společností po celém světě, kterým pomohl k větší efektivitě pracovních postupů. Tohle spojení jednoznačně ukázalo skutečnost, že použití blockchainu neslouží pouze kryptoměnám, ale lze jej použít i v tak komplikovaném a náročném odvětví jako je lodní doprava. [24]

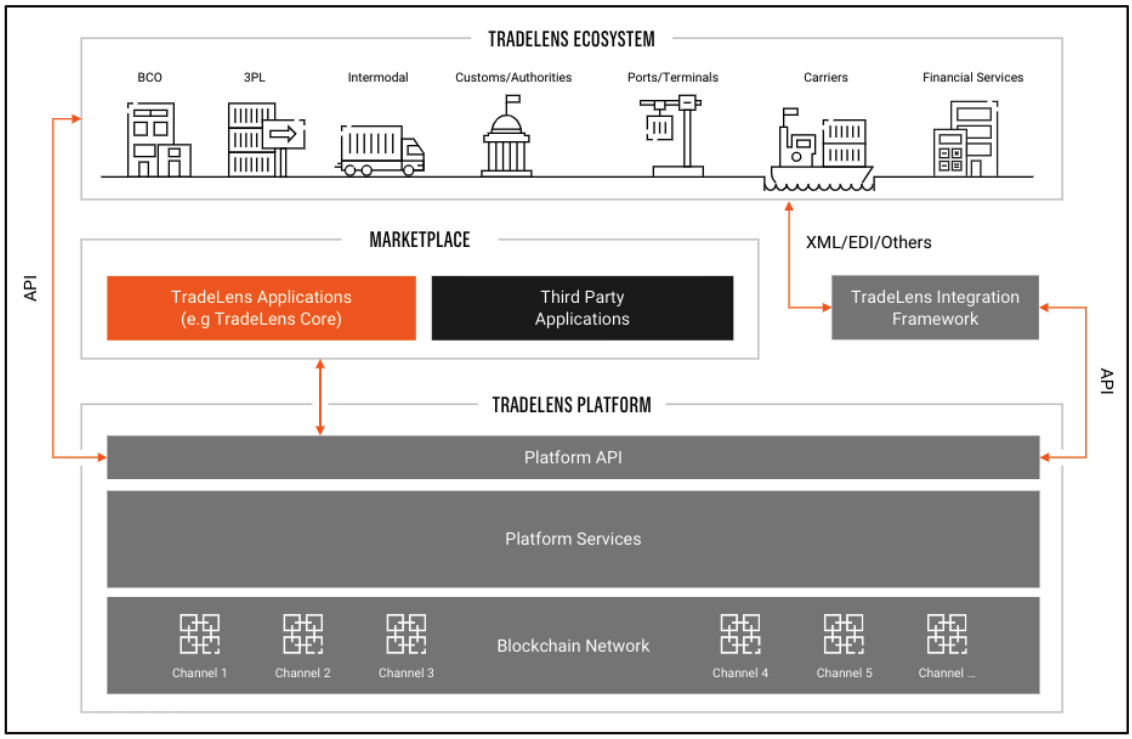
Odvětví lodní dopravy se dlouhodobě potýká s různými problémy. Řada přepravních a logistických společností má své procesy závislé na zastaralých systémech a není možné se vyhnout velkému množství papírování a byrokracii. Přeshraniční přeprava mnohdy zahrnuje ruční ověřování papírových dokumentů u každé zásilky. Například chlazené zboží, které je přepravováno z východní Afriky do Evropy, musí projít přibližně přes 30 lidí nebo organizací, než dorazí na místo určení. Tyto procesy jsou časové náročné a mohou zvyšovat chybovost. Výsledkem může být ztráta dokumentace nebo zpožděné doručení. Tyto zmiňované problémy se společnost Maersk spojením s IBM rozhodla řešit a proto představily multifunkční platformu TradeLens. [24]

Cílem platformy TradeLens je zajistit bezpečné sdílení informací, zajistit větší spolupráci napříč dodavatelskými řetězci a podpořit větší transparentnost a efektivitu globálního obchodu. TradeLens poskytuje všem účastníkům transakce jednotný pohled na sdílené přepravní údaje. Odesílatelé, speditéři, provozovatelé terminálů a přístavů, celní orgány a další články dodavatelského řetězce spolu mohou efektivně komunikovat. Všichni se během přepravy dostanou na detaily přepravních dokumentů, současně k datům získaným prostřednictvím Internetu věcí a senzorů, které kontrolují teplotu, hmotnost kontejneru apod. [24]

Architektura platformy TradeLens

Cele řešení se skládá ze tří základních částí – ekosystému, platformy a tržiště. Projekt TradeLens zahrnuje účastníky transakce, jako jsou námořní dopravci, přístavy, zprostředkovatelé přepravy, celní orgány a další související strany, kteří se připojují k platformě,

poskytují jí data a používají ji. Platforma je přístupná prostřednictvím otevřeného rozhraní Application Programming Interface (API)[1] a spojuje účastníky transakce. Umožňuje sdílet informace a spolupracovat. Platforma běží v cloudu společnosti IBM a využívá open-source blockchainové technologie Hyperledger Fabric pro zabezpečení dat. Tržiště umožňuje třetím stranám vyvíjet a nasazovat různé aplikace vhodné pro daný účel na platformě TradeLens. [25]



Obr. 2.1: Architektura platformy TradeLens, Zdroj: [25].

Přestože se projekt TradeLens osvědčil, čelí konkurenci některých dalších konsorcií, poskytovatelů technologií a dokonce i startupů. Přirozeně všichni chtějí zlepšit dodavatelské řetězce a pomoci dopravním a logistickým společnostem zbavit se rutinních procesů.

2.3.2 Global Shipping Business Network (GSBN)

Global Shipping Business Network (GSBN) je konsorcium, které založil poskytovatel softwaru pro správu zásilek CargoSmart spolu se světoznámými námořními dopravci, jako jsou Compagnie Maritime d'Affrètement and Compagnie Générale Maritime (CMA CGM) (Francie), China Ocean Shipping Company (COSCO) (Čína), Evergreen Marine

[1] Jde o sbírku procedur, funkcí, tříd či protokolů nějaké knihovny, které může programátor využívat. API určuje, jakým způsobem jsou funkce knihovny volány ze zdrojového kódu programu.

(Tchaj-wan) a Orient Overseas Container Line (OOCL) (Hongkong). Dále sem patří přístavy Hutchison Ports (Rotterdam v Nizozemí) a Shanghai International Port v Číně. GSBN dává odesílatelům možnost digitalizace a automatizace dokumentace. Má také řešení pro nakládání se zbožím, které je klasifikováno jako nebezpečné a podléhá řadě předpisů. Dalším cílem GSBN je zajistit bezproblémové sdílení a výměnu dokumentů včetně dalších informací ve všech fázích přepravního procesu. [24]

2.3.3 Oracle Supply Chain Management (Oracle SCM)

Jedním z konkurentů projektu TradeLens je Oracle Supply Chain Management (Oracle SCM) od společnosti Oracle, který poskytuje sadu aplikací s otevřenou a mimořádně flexibilní architekturou. Nabízí integrované a modulární možnosti nasazení. Společnost Oracle nabízí řadu řešení skladování, řízení dopravy a globálního obchodu, správy vozového parku a logistiky. Vzhledem k tomu, že řešení Oracle SCM je otevřené, integrované a kompletní, může pomoci transformovat různé přepravní operace a zefektivnit i ty nejnáročnější a nejkomplikovanější procesy dodavatelského řetězce. [24]

2.3.4 Platforma Smart B/L

Slovinský startup CargoX buduje vlastní platformu Smart B/L pro ověřování konosamentů[2]. Toto řešení umožní dopravcům vystavovat a převádět elektronické konosamenty digitálně, bezpečně a bez padělání v otevřeném prostředí. Podle společnosti CargoX bude její řešení vhodné pro spediční společnosti a dopravce neprovozující plavidla. [24]

2.3.5 Použití v železniční dopravě

Železniční společnost Canadian Pacific se nedávno připojila k TradeLens, v rámci procesu dokumentace transkontinentální železnice. Má tratě v Kanadě a USA s přímým spojením s hlavními přístavy na západním a východním pobřeží. Společnost Canadian Pacific očekává, že platforma urychlí sdílení dokumentů s ostatními účastníky dodavatelského řetězce u intermodálních dopravců, kteří propojují lodní dopravu se silniční. Železniční společnost Canadian Pacific je desátým intermodálním dopravcem, který se připojil k projektu TradeLens. [26]

[2]Konosament, jinak náložný list (angl. bill of lading, B/L), je cenný papír a dopravní dokument, používaný při přepravě nákladu po moři.

2.4 Platforma ElA blockchain

Platforma ElA blockchain je projekt Elektrotechnické asociace České republiky (nestátní nezisková organizace zaměstnavatelů). Jedná se o průmyslový blockchain, který je tvořen konsorciem několika subjektů, tzv. konsorciální blockchain. Podobně jako TradeLens, pro svůj provoz využívá blockchainovou open-source platformu Hyperledger Fabric.

Platformu ElA blockchain buduje komunita soukromých firem a státních institucí pro vlastní potřeby ověřování dokumentů v digitální podobě. Platforma ElA blockchain má svou vlastní síť uzlů (nodů), která je veřejná a otevřená, ale není anonymní. Provoz sítě, bezpečnost a stabilitu má na starosti firma, která byla pro tento účel založena, ELA Blockchain Services, a. s. Připojit si vlastní uzel do sítě je umožněno pouze důvěryhodným právnickým osobám, které ELA Blockchain Services, a. s. schválila a garantuje tím jejich důvěryhodnost. Poskytne jim tzv. identitu – elektronický certifikát opravňující k operacím na svém blockchainu.

Narozdíl od platformy TradeLens, kterou buduje konsorcium Maersk a IBM, a která je dále poskytována svým partnerům, je platforma ElA blockchain nezávislá, tzn. že nemá centrálního zřizovatele. Funguje na bázi dobrovolného sdružení majitelů uzlů (nodů), kterými jsou schválené právnické osoby.

Do projektu jsou zapojeni různí vlastníci převážně z České republiky, a také známé instituce jako např. Ministerstvo průmyslu a obchodu nebo Hospodářská komora České republiky. Seznam majitelů uzlů je veřejně dostupný, takže si uživatel může vybrat majitele, kterému více důvěřuje viz následující obrázek 2.2. [27]

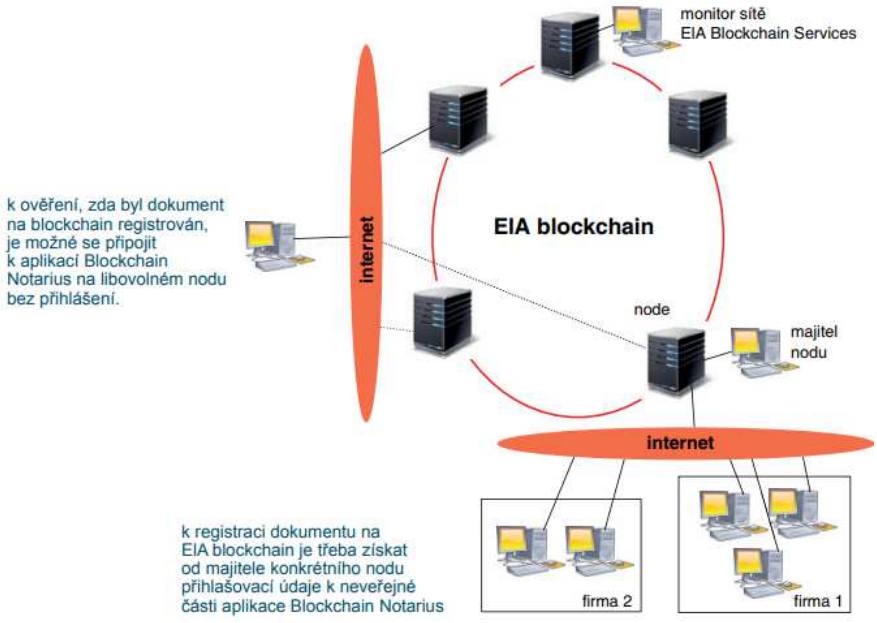
Seznam poskytovatelů služby Blockchain Notarius. U kteréhokoliv z nich lze zdarma ověřit již registrovaný dokument. K samotné registraci dokumentu je nutné získat od majitele nodu přístup k neveřejné části aplikace Blockchain Notarius. Tato služba může být majitelem nodu zpoplatněna.

Zobrazeno 20 odkazů Vyhledávání:

Název nodu	Vlastník nodu	Sídlo majitele	Kontakt	Dostupnost	Přejít
TUV	TÜV SÜD Czech	Česká republika	jan.vrana@tuv-sud.cz		Odkaz
MPO	Ministerstvo průmyslu a obchodu	Česká republika	rehak@mpo.cz		Odkaz
SPCR	Svaz průmyslu a dopravy České republiky	Česká republika	oferdus@spcr.cz		Odkaz
CL	Černý Legal	Česká republika	cerny@cernylegal.com		Odkaz
KMX	KOMIX s.r.o.	Česká republika	jancek@komix.cz		Odkaz
UNC	uniCORE, s.r.o.	Slovenská republika	peter.pikna@unicore.sk		Odkaz
MULT	MULTIMA a.s.	Česká republika	anovotny@multima.cz		Odkaz
AICK	AI check	Česká republika	ondrej.ferdus@aicheck.tech		Odkaz
NXP	NEXPRO Communication s.r.o	Česká republika	lenka.cilova@nexpro.cz		Odkaz
EBS-JPN	ELA Blockchain Services a.s.	Česká republika	kozak@elachain.cz		Odkaz
HKCR	Hospodářská komora České republiky	Česká republika	kaspar@komora.cz		Odkaz
UTB	Univerzita Tomáše Bati ve Zlíně	Česká republika	dmalanik@utb.cz		Odkaz

Obr. 2.2: Příklad seznamu uzlů platformy ElA blockchain, Zdroj: [28].

Jedna právnická osoba smí vlastnit pouze jeden uzel (node). Toto pravidlo zajišťuje odolnost proti technickému selhání nebo hackerskému útoku a také proti zneužití dominantním subjektem. Platforma ElA blockchain je otevřená jakémukoliv typu aplikace a nezaměřuje se na konkrétní použití. V základní verzi obsahuje aplikaci pro registraci digitálních dokumentů Blockchain Notarius. [27]



Obr. 2.3: Popis platformy ElA blockchain, Zdroj: [27].

Princip platformy ElA blockchain je vidět na obrázku 2.3. Znázorňuje princip fungování aplikace Blockchain Notarius. Uzly (nody) schválených institucí dohromady tvoří blockchainovou síť. Prostřednictvím sítě internet je možné s platformou ElA blockchain komunikovat. ElA blockchain umožňuje provádět dvě základní transakce: registraci a ověření digitálního souboru. Jak již bylo zmíněno dříve, do blockchainu se neukládají dokumenty, nýbrž pouze jejich digitální otisky, tzv. heše. Pro registraci digitálního souboru je nutné mít přístup do privátní části aplikace Blockchain Notarius. Každý majitel uzlu (nodu) může digitální soubory sám registrovat a poskytuje přístup k aplikaci. Vpravo dole *firma 1*, *firma 2*, to jsou ti, kterým majitel uzlu (nodu) přidělil přístup a mohou registrovat digitální soubory i když nemají vlastní uzel (node). Ověřit si registraci digitálního souboru je možné z jakéhokoliv uzlu (nodu), v rámci veřejné části aplikace Blockchain Notarius, viz vlevo uprostřed.

2.4.1 Aplikace Blockchain Notarius

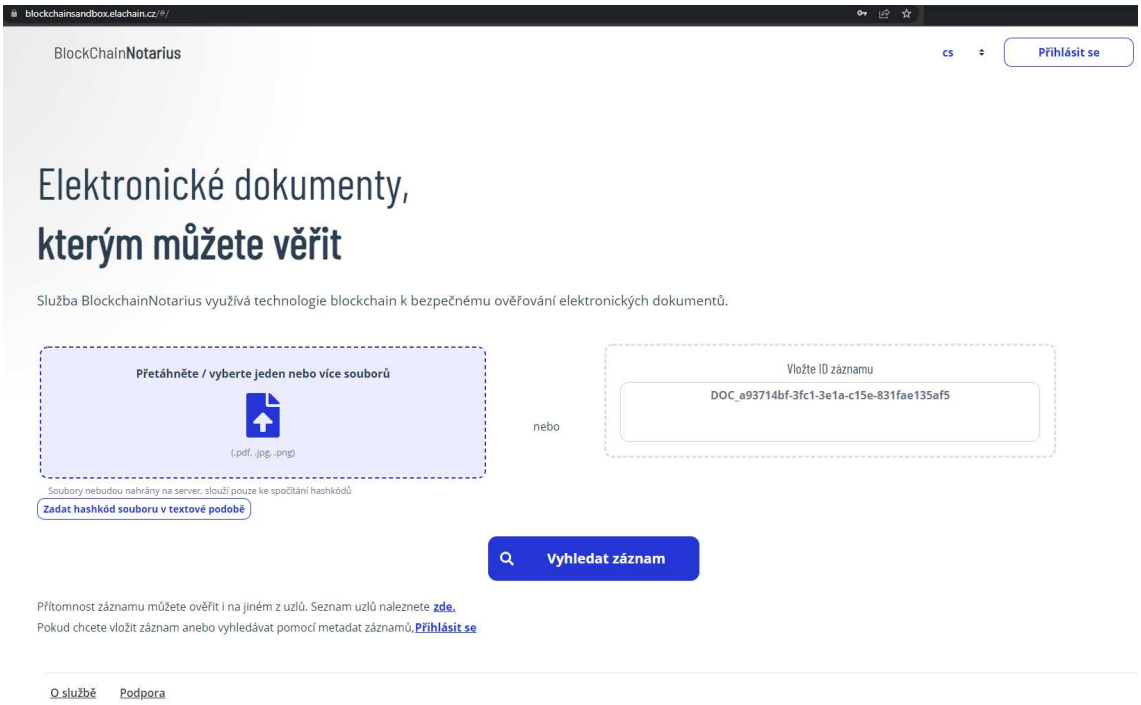
Blockchain Notarius® je chráněná obchodní značka společnosti ELA Blockchain Services a.s., která je dceřinou společností Elekrotechnické asociace České republiky. Aplikace umožňuje ověřování identity datových souborů, uzavírání smluv a potvrzování pravosti záznamů. Je povinně instalována ve všech uzlech ElA blockchainu. Každý, kdo se rozhodne si uzel pořídit, má aplikaci zdarma a může tím pádem registrace do blockchainu nabídnout (komerčně) i těm, kteří uzel nemají. Aplikace Blockchain Notarius má ambice dobýt světový trh, proto je k dispozici ve více jazykových mutacích, kromě češtiny a angličtiny, také v taiwanské a zjednodušené čínštině. Japonská jazyková mutace se připravuje. [27]

Společnost ELA Blockchain Services a. s. nabízí možnost vyzkoušet si zkušební verzi aplikace Blockchain Notarius, která je dostupná na blockchainsandbox.elachain.cz, této možnosti jsem využil a dále ji popíši.

Aplikace se skládá ze dvou částí, veřejné a privátní.

Veřejná část aplikace

Veřejná část aplikace umožňuje kontrolu registrovaného datového souboru. Není vyžadováno přihlášení a každý vlastník uzlu (nodu) je povinen poskytnout přístup do ní zdarma. Je běžně přístupná prostřednictvím webových stránek platformy www.elachain.cz.

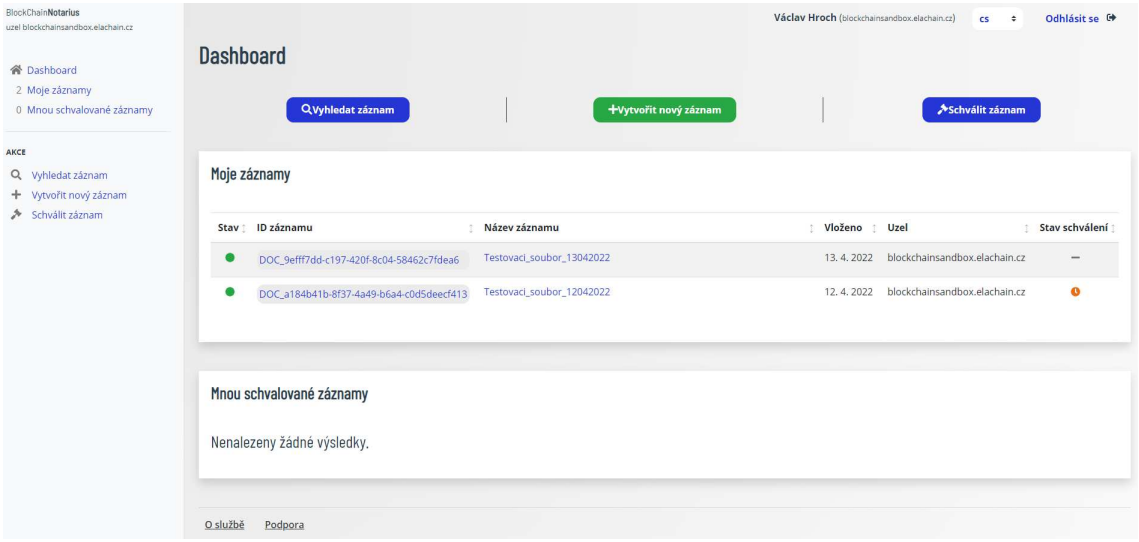


Obr. 2.4: Veřejná část aplikace Blockchain Notarius, Zdroj: [27].

Kontrolu registrace digitálního souboru provedeme buď vložením kontrolovaného souboru a vypočtením jeho heše (levá část) nebo vložením identifikačního čísla záznamu (pravá část), které je automaticky vygenerováno v privátní části aplikace Blockchain Notarius při registraci souboru.

Privátní část aplikace

Privátní část aplikace umožňuje registraci libovolného datového souboru (text, obrázek, fotka, audio, video atd.). Přístup k ní má majitel uzlu (nodu) a osoby, kterým poskytne přístupová práva. Následující obrázek 2.5 ukazuje hlavní nabídku privátní části aplikace, která je dostupná po zadání přihlašovacích údajů (emailová adresa a heslo).



Obr. 2.5: Privátní část aplikace Blockchain Notarius, Zdroj: [27].

Na hlavní stránce je zobrazení přehledu mých záznamů, mnou schválených záznamů a seznam tří akcí, které mohu provádět. Za prvé mohu vyhledat záznam, za druhé vytvořit záznam a za třetí záznam schválit. Mohu schvalovat záznamy ostatních nikoliv však vlastní záznamy. Tohle je speciální funkce aplikace Blockchain Notarius. Umožňuje schválení registrovaného dokumentu ještě dalším účastníkem kontraktu. Smlouva se schválením je v blockchainu registrována jako schválená oběma partnery. Záznamy je možné schválit na libovolném uzlu (nodu) ElA Blockchain sítě, po zadání dvou zabezpečovacích prvků (identifikačního čísla a PIN) zaslaných autorem smlouvy. [27]
Příklady možného použití aplikace Blockchain Notarius:

- registrace firemních dokumentů,
- registrace autorského díla,
- důkaz stavu v předmětném okamžiku (např. měřicí protokoly),
- vzdálené uzavření smlouvy,
- ověřování certifikátů. [27]

2.4.2 Prosazení platformy ElA blockchain v Asii

Od 6. ledna roku 2021 je platforma ElA blockchain součástí cloudové platformy WISE-PaaS, kterou pro své partnery a zákazníky provozuje taiwanská technologická společnost Advantech Co. Na rozdíl od české verze aplikace Blockchain Notarius, která je nabízena

zdarma, tak v Asii je zpoplatněna. Následujícím projektem společnosti Advantech Co., je využití ElA blockchainu v ověřování a ochraně medicinských dat, což je zejména v Japonsku velmi citlivé téma. [27]

2.4.3 Použití v systémech řízení kvality

Na základě požadavku Rady kvality České republiky byla vypracována *Studie k využití blockchainových technologií v systémech řízení kvality*. Tuto studii vypracovala Elektrotechnická asociace – servis s. r. o. Rada kvality České republiky je orgánem vlády České republiky, která je zřízena na podporu rozvoje řízení a uplatňování Národní politiky kvality. Řízení Rady kvality České republiky má na starost Ministerstvo průmyslu a obchodu České republiky. Pro zajištění důvěryhodnosti blockchainové technologie musí být důvěra zaváděna mezinárodně. Mezinárodní organizace pro normalizaci (International Standardization Organization (ISO)) v roce 2016 zřídila komisi ISO / TC 307 pro vývoj norem v oblasti blockchainu. Na tvorbě těchto norem se podílí více jak 40 zemí z celého světa. Dále se studie zabývala možnostmi využití blockchainových technologií při akreditaci a v certifikačních systémech. Cílem studie bylo představit technologii blockchain laické veřejnosti a vhodně informovat o významu použití průmyslového blockchainu pro zajištění kvality výroby či služeb. [29]

2.4.4 Ověřování vysokoškolských diplomů

V České republice zatím běží pár projektů na průmyslovém blockchainu společnosti ELA Blockchain Services, a. s., nicméně si myslím, že v budoucnu se počet blockchainů, vlivem větší digitalizace a tlaku na ekologii (méně papírování), bude rozšiřovat.

Dalším projektem je aplikace Diplomachain. Digitalizace má člověku především pomáhat, ale také může být v některých případech na škodu. Vzhledem k dostupnosti grafických programů je velmi snadné vyrobit si falešný diplom např. z vysoké školy, kde na první pohled nemusí být vůbec jasné, zda je pravý nebo falešný. Diplomachain je aplikace, která zajistí ověřování dokumentů a běží na blockchainu.

Její funkce ve třech krocích:

1. vzdělávací instituce uloží heš dokumentu (diplomu) do aplikace,
2. absolventovi je předán dokument běžným způsobem,
3. kdokoliv a kdekoliv si může ověřit pravost souboru.

V aplikaci Diplomachain nejsou uloženy soubory s dokumenty, ale pouze jejich heše, které jsou pro každý soubor unikátní. [30]

2.4.5 Digitální potvrzení bezinfekčnosti

Koncem roku 2019 se v Číně začaly objevovat první případy neznámého vysoce infekčního respiračního onemocnění. To se postupně mnohdy nekontrolovaně rozšířilo po celém světě. Řeč je o stále trvající celosvětové koronavirové pandemii způsobující onemocnění **CO**rona**VI**rus **D**isease 20**19** (COVID-19). Problém této nemoci je vysoká infekčnost ještě před propuknutím a většinou bez známky únavy či jakýchkoliv příznaků, jako jsme byli zvyklí u běžných respiračních onemocnění. Postupným vývojem pandemie se ukázalo, že je potřeba populaci pravidelně testovat a nakažené jedince izolovat. Z počátku roku 2020 tam kde to bylo možné byla nařízena práce z domova. V případě nutnosti docházet na pracoviště se musel pracovník prokázat negativním testem. Vládní opatření se v průběhu pandemie již několikrát různě měnila, především v návaznosti na její vývoj. To způsobovalo zaměstnavatelům vyšší míru administrativní zátěže a bylo na nich, jak si s tím dokáží poradit. Zde vznikl tlak na vyšší míru digitalizace a využití informačních technologií ve větší míře než jsme doposud byli zvyklí.

Možnosti digitalizovat využila brněnská společnost Enbra, a. s., která se zabývá vytápěním, chlazením a měřením spotřeby vody. Začátkem května roku 2020, jako první v České republice, spustila projekt digitálního prohlášení o bezinfekčnosti. Zareagovala tím tak na rozvolnění vládních opatření, která umožnila postupný návrat lidí na svá pracoviště. Jednoznačně to byla příležitost, jak se vyhnout časově náročné administrativní zátěži, kterou by sebrala kontrola papírových prohlášení s ohledem na počet přibližně stopadesát zaměstnanců. Prostřednictvím jednoduchého webového rozhraní může zaměstnanec učinit čestné prohlášení za několik vteřin, pohodlně cestou do práce z mobilního zařízení. Tím se eliminují ranní fronty, které se u některých společností mohou tvořit nejčastěji u vstupu do budovy, na vrátnici nebo recepci. Řešeny jsou v tomto ohledu i schůzky mimo firmu, které absolvují např. obchodní zástupci. Digitální prohlášení vyplňují nejen zaměstnanci, ale jejich prostřednictvím také zákazníci. Podobně i další cizí zaměstnanci vstupující do prostorů společnosti Enbra. Riziko přenosu nákazy se s tímto přístupem snižuje na minimum. S dodavatelem této technologie společnost pracuje na dalším vylepšení, které spočívá ve využití QR kódů instalovaných do mobilních telefonů zaměstnanců. [31]

Tato digitalizace je pilotním projektem společnosti ELA Blockchain Services, a. s., která prosazuje decentralizaci a provozuje první průmyslový blockchain v České republice. Jak to celé funguje, lze jednoduše shrnout do několika kroků. Zaměstnanec se nejprve identifikuje, poté učiní (odklikne) čestné prohlášení o bezinfekčnosti. Následně je vypočítán heš tohoto prohlášení a je zapsán navždy do blockchainu. Jak už víme z teorie, není možné zpětné zfalšování a ani není možné určit jméno zaměstnance nebo název firmy. V případě potřeby se k citlivým osobním údajům dostane pouze pověřený pracovník (personalista). Papírová prohlášení mohou být dodatečně upravována, což v případě použití blockchainu nelze. Je důležité zmínit, že v rámci blockchainu se ukládají pouze heše, ostatní citlivá data zůstávají ve vlastnictví a úložištích příslušné společnosti. [31]

2.5 Chytré kontrakty (Smart contracts)

Chytré kontrakty (z angl. Smart contracts) bývají překládány několika různými spojeními, ale vždy se jedná o tu samou věc – chytré kontrakty, chytré smlouvy nebo inteligentní smlouvy.

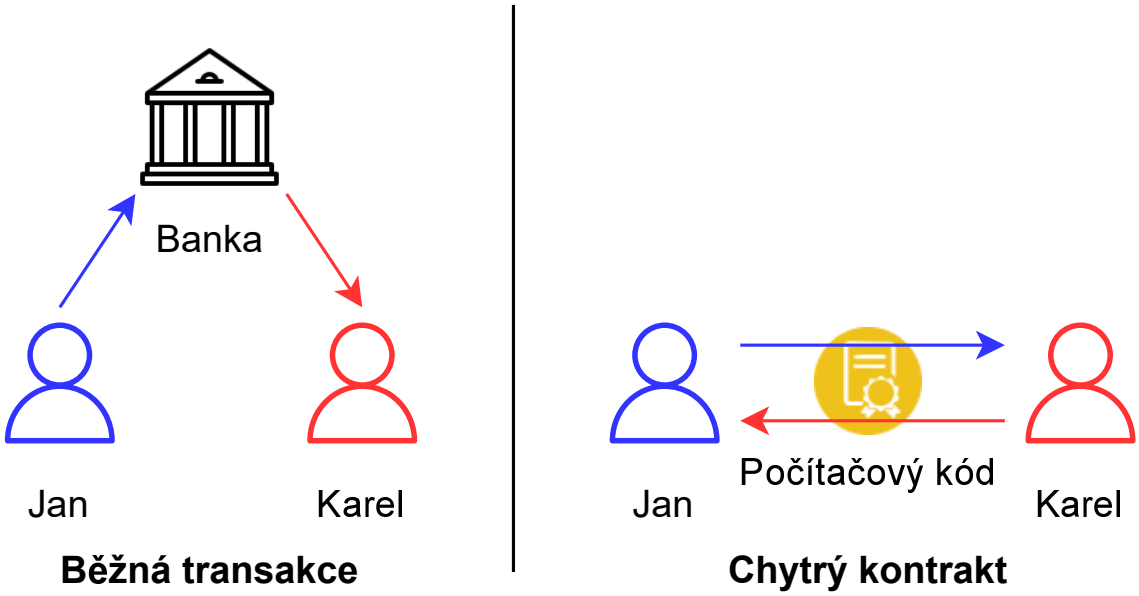
Fungování chytrých kontraktů bylo poprvé představeno v roce 1994 Nickem Szabem, americkým počítačovým expertem. O čtyři roky později, v roce 1998 vynalezl virtuální měnu nazvanou Bit Gold. Přesně deset let před vynálezem Bitcoinu. Možná proto je Nick Szabo často „podezříván“, že je skutečný Satoshi Nakamoto. Definoval chytré kontrakty jako „počítačové transakční protokoly, které splňují podmínky smlouvy“. [32]

Chytré kontrakty však zůstaly poměrně dlouho v zapomnění a nedařilo se k nim přitáhnout pozornost průmyslu a akademické obce, protože před vznikem technologie blockchain v roce 2009 neexistovala žádná platforma pro provozování chytrých smluv. [33]

Chytré kontrakty se znovu objevily až s příchodem kryptoměny Ethereum.

Využívají protokol nebo software, kterým lze nahradit standardní smlouvy v papírové podobě. Stejně jako papírová verze, tak i elektronické verze chytrých kontraktů zaznamenávají podmínky smlouvy a dokáží si vynutit jejich vykonání. Odstraňují nutnost existence papírové smlouvy uzavřené mezi dvěma smluvními stranami. [32]

Pro názornou ukázku slouží obrázek 2.6, kde je vidět rozdíl, jak funguje běžná transakce s využitím třetí strany (banka), mezi dvěma zákazníky Janem a Karlem (smluvními stranami), a chytrý kontrakt, kde je absence třetí strany (banky) a podmínky jsou řešeny v rámci počítačového kódu.



Obr. 2.6: Běžná transakce vs chytrý kontrakt, Zdroj: [34], vlastní zpracování.

V úplně prvním návrhu chytrých kontraktů Szabo popsal použití na běžně obchodovaných aktivech jako jsou deriváty (např. cenné papíry, komodity) a dluhopisy. Předpověděl, že velmi složité termínované struktury pro platby mohou být nyní zabudovány do standardizovaných smluv a obchodovány s nízkými transakčními náklady. Hodně z předpovědí v Szabově dokumentu (whitepaperu), sice předběhly o mnoho let technologii blockchainu, a i přesto se potvrdily. Obchodování s deriváty je dnes většinou prováděno prostřednictvím počítačových sítí s využitím komplexních termínovaných struktur, tak jak dokument předpovídal. [32]

2.5.1 Popis principu chytrého kontraktu

Představit si fungování chytrého kontraktu lze na jednoduchých příkladech.

Nápojový automat

Vhodíte minci a dostanete nápoj nebo vám jsou vráceny peníze. Aby vše správně fungovalo, je v nápojovém automatu program (software), který kontroluje pravost mincí, výši vhozené částky, storno objednávky a případné vrácení přeplatku. Tento program si lze představit jako chytrý kontrakt, který komukoliv s dostatečným množstvím hotovosti garantuje, že dostane nápoj za předem stanovenou částku. [32]

Předplacená SIM karta

Jestliže máme na SIM kartě dostatečný kredit, můžeme využívat služby nabízené mobilním operátorem v plném rozsahu. Jakmile klesne kredit pod vyžadovanou výši, jsou služby pozastaveny a uživatel je informován o nedostatečné výši kreditu. Vše probíhá automaticky. [32]

2.5.2 Výhody

Přesnost

Jedním z nutných požadavků u chytrých smluv je podrobně zaznamenat všechny podmínky. Bez dodržení přesnosti může docházet k transakčním chybám. [35]

Transparentnost

Smluvní podmínky jsou viditelné a přístupné všem stranám. Jakmile je smlouva uzavřena, nelze ji nijak zpochybnit. To umožňuje úplnou transparentnost transakce pro všechny zúčastněné strany. [35]

Bezpečnost

Smlouva je zašifrovaná a distribuovaná mezi uzly. Nemůže být jednoduše ztracena či změněna bez svolení jejího uživatele narozdíl od běžné papírové smlouvy. [35]

Hospodárnost a rychlost

Chytré kontrakty běží v softwarovém kódu a jsou k dispozici na internetu. Díky tomu lze provádět transakce velmi rychle. To může ušetřit mnoho hodin oproti tradičním obchodním procesům. Není totiž třeba ručního zpracování dokumentů. Z hlediska hospodárnosti nezatěžují chytré kontrakty životní prostředí a mohou být tzv. „zelené“, protože fungují virtuálně, odpadá nutnost spotřeby hromady papírů. [35]

Efektivita

Díky rychlosti a přesnosti se přirozeně projeví efektivita těchto smluv. Vyšší efektivita má za následek zpracování většího počtu transakcí vytvářejících hodnotu za jednotku času. [35]

Standardizace

Existuje již několik druhů chytrých smluv, ze kterých je možno vybrat si tu nejvhodnější a využít ji podle svých potřeb. [32]

2.5.3 Nevýhody

Nejistý právní status

Zatím neexistuje úprava v právním systému, která by konkrétně upravovala využívání chytrých kontraktů. [36]

Náklady na implementaci

Pro využití chytrých smluv je potřeba znalost příšlušného programovacího jazyka a nutnost korektní implementace kontraktu, protože transakce v blockchainu jsou nevratné. [36]

Odstoupení od smlouvy

Chytré smlouvy jsou doslovné, neexistuje tedy způsob, jak je zrušit, což byste mohli udělat s tradiční smlouvou, např. u soudu. [36]

Lidský faktor

Jakmile je chytrá smlouva zanesena do blockchainu, je neměnná. V případě, že člověk na začátku ve smlouvě udělá chybu, obtížně se napravuje.

2.5.4 Potenciál využití

Chytré kontrakty mají potenciál využití v různých odvětvích:

- logistický řetězec – efektivní správa zásilek,
- finanční sektor – systém správy finančních půjček,
- řízení zdravotní péče,
- státní sektor – zadávání veřejných zakázek. [33]

3 Návrh systémového využití platformy Blockchain v oblasti průmyslových transakcí

Možná zásluhou velké popularity kryptoměn, ze kterých se přirozeně vyvíjí další technologie, je stále větší zájem o inovace a digitalizace procesů v průmyslových podnicích. S tím se zvyšuje zájem o využití technologie blockchainu. Případné využití v průmyslových podnicích však má specifické požadavky na výkon a konkrétní aplikace blockchainové technologie se může v závislosti na druhu podniku lišit. Na rozdíl od kryptoměn, je pro průmyslové použití potřeba zohlednit řadu požadavků ještě před návrhem systému.

3.1 SWOT analýza blockchainové technologie

Před návrhem systému je dobré shrnout jeho výhody a nevýhody, které by nás mohly později nemile překvapit. Pro přehlednost jsem použil SWOT analýzu. Zkratka se skládá z prvních písmen čtyř anglických slov **S**trenghts, **W**eaknesses, **O**pportunities, **T**hreats (SWOT). V překladu se SWOT analýza zabývá silnými a slabými stránkami zkoumaného projektu (podniku), jeho příležitostmi a hrozbami.

Následující tabulka 3.1, shrnuje teoretické vlastnosti blockchainové technologie probírané v předchozích kapitolách do ucelené tabulky.

Tab. 3.1: SWOT analýza blockchainové technologie

Silné stránky (S)	Slabé stránky (W)
Decentralizace sítě	Zabezpečení soukromí dat (veřejná vs privátní síť)
Transparentnost dat	Malá nebo žádná uživatelská zkušenost
Robustní architektura	Neměnnost provedených transakcí
Rychlý přístup k transakcím	Omezená škálovatelnost
Historie transakcí v distrib. účetní knize	Změna legislativy
Příležitosti (O)	Hrozby (T)
Chytré kontrakty	Opatrnost k přijímání nových technologií
Eliminace důvěry třetích stran	Náchylnost k bezpečnostním útokům
Snížení rizika podvodu	Snížení zaměstnanosti v různých odvětvích

Zdroj: Vlastní zpracování

3.1.1 Shrnutí SWOT analýzy

Silné stránky (S) a příležitosti (O) jsem se snažil popsat v předchozích odstavcích, proto zde podrobněji popíši pouze slabé stránky a hrozby.
Slabé stránky (W):

- zabezpečení soukromí dat – ne vždy je vhodné vše sdílet,
- malá nebo žádná uživatelská zkušenost – technologie je poměrně nová a většinou probíhá teprve testování,
- neměnnost provedených transakcí – omezuje pozdější úpravu uživatelských dat,
- omezená škálovatelnost – závisí na použitém konsenzuálním algoritmu konkrétní platformy,
- změna legislativy – technologie blockchain zatím nemá právní oporu.

Hrozby (T):

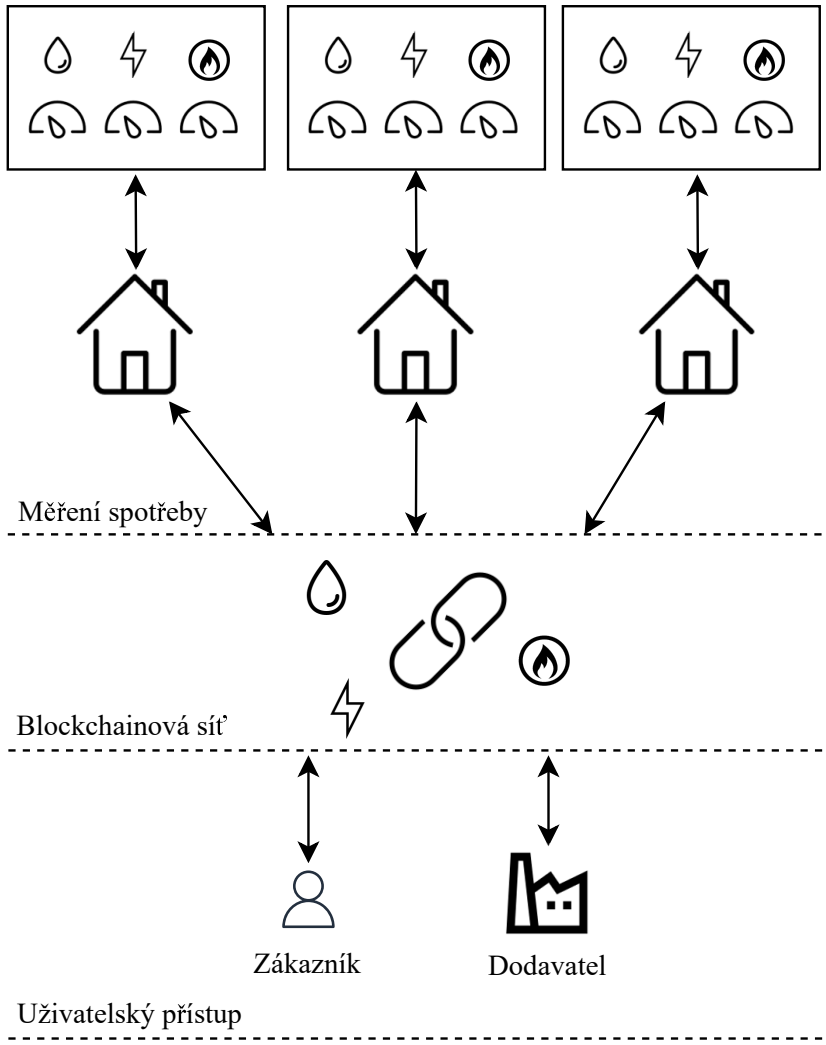
- opatrnost k přijímání nových technologií,
- náchylnost k bezpečnostním útokům – vše je digitální (jednodušší zneužití),
- snížení zaměstnanosti v různých odvětvích – rušení pracovních míst.

3.2 Návrh využití platformy Blockchain v energetickém průmyslu

Výhoda ověřených zpětně nezměnitelných údajů by mohla najít využití v energetickém průmyslu. Budu zde uvažovat typické bydlení, kdy veškeré energie potřebné pro chod domácnosti, většinou elektřinu, vodu a někdy i zároveň plyn, odebíráme od externích dodavatelů. Každý dodavatel, který nám energii dodává, potřebuje mít přehled, jaké množství energie jsme odebrali. Zejména proto, aby nám ji mohl naúčtovat a také aby mohl lépe plánovat budoucí nákupy energií pro svoje zákazníky (domácnosti, firmy).

Současné systémy monitorování spotřeby umožňují manipulaci s měřidly, která vede k nesprávným záznamům měřených údajů (černé odběry, falšování naměřených údajů) a tím dochází k poškozování dodavatelů energií, kde může docházet k finančním ztrátám.

Návrh využití platformy blockchain je znázorněn na obrázku 3.2, který umožňuje lepší porozumění principu zamýšleného fungování celého systému.



Obr. 3.2: Návrh využití platformy blockchain, vlastní zpracování.

Navrhovaný systém se skládá ze tří částí: měření spotřeby, blockchainové sítě a uživatelské části.

Při popisu shora – na začátku je centrální zařízení, které sesbírá data ze všech měřidel v domácnosti, v tomto případě voda, elektřina a plyn, a zaznamenaná data zpracuje. Následně jsou data z centrálního zařízení (terminálu) přenesena do blockchainové sítě, ve které jsou zapojeny energetické společnosti, pro jejich ověření a uložení. Současně každý dodavatel energií umožňuje komunikaci se zákazníkem prostřednictvím uživatelské části aplikace a blockchainové sítě, pro zprostředkování dotazů a požadavků souvisejících s provozem. Zde si dovolím upozornit, že toto řešení nebere ohled na konkurenci jednotlivých energetických společností a zabezpečení sdílení dat.

4 Vyhodnocení vlastního návrhu a možnosti aplikačního nasazení

Zajištění správnosti a zpětné nezměnitelnosti naměřených údajů při odečtu energií je přínosné pro celou společnost. Technologie blockchain a její specifické vlastnosti přináší do této oblasti nové možnosti řešení. Jednou z neopomenutelných výhod blockchainu, je schopnost zaznamenat důkaz v předmětném okamžiku, a to je při tomto řešení odečtu odebraného množství energií velmi vhodné.

Navrhovaný systém se zabývá sběrem a následným sdílením naměřených údajů s využitím blockchainové sítě. Navrhovaná koncepce by v praktickém použití mohla narazit na problematiku sdílení dat mezi energetickými společnostmi, především kvůli konkurenci. I přesto si myslím, že v tomhle ohledu sběru a distribuce naměřených dat, může být využití blockchainu přínosné.

Možná technická omezení blockchainu závisí na konkrétní aplikaci a použité platformě, protože výkony jednotlivých platforem se od sebe velmi liší. Případy použití, které vyžadují extrémně rychlé transakce (v řádu milisekund), nejsou pro blockchainové systémy vhodné, protože jejich výkon je mnohem pomalejší v závislosti na použitých konsenzuálních algoritmech.

4.1 Možnosti aplikačního nasazení

Vzhledem k rostoucí popularitě elektromobility je zde možná příležitost využití chytrých kontraktů pro distribuci elektrické energie. V případě domácí výroby elektrické energie, např. pomocí solárních panelů na střeše domu. Výrobce (domácnost) by mohl nabízet přebytečnou vyrobenou energii s cenou určenou podle aktuální situace na energetickém trhu v reálném čase např. svému sousedovi, který by ji následně použil k dobití energie ve svém elektromobilu.

Dalším využitím by mohla být možnost zápisu přesného počtu najetých kilometrů v případě pravidelné technické kontroly vozidla a tím pádem příležitostí, jak snadno a efektivně zabránit případným podvodům se stočenými kilometry.

Všechny zmiňované případy se zabývají důkazem v předmětném okamžiku, proto si myslím, že je použití technologie blockchain vhodné.

Závěr

Blockchain a jemu příbuzné technologie jsou oceňovány pro svou decentralizovanou infrastrukturu. S kryptoměnami, které jejich význam uvedly ve známost, je však spojována řada nelegálních aktivit, např. praní špinavých peněz, objednávky trestné činnosti, nákup zbraní, drog apod. To ve výsledném efektu zavádění blockchainu nepomáhá.

Cíl práce se podle mého mínění podařilo splnit. Nejprve jsem se zaměřil na popis principu fungování technologie blockchain. Následně jsem se zabýval současnými možnostmi využití v logistických procesech včetně příkladů použití. Na to jsem navázal možností vyzkoušet a ověřit si, jak funguje skutečná aplikace blockchainové technologie v reálném světě. Vyzkoušel jsem blockchainovou platformu ElA a jejich aplikaci Blockchain Notarius®. Popsal jsem základní princip fungování a teoretické možnosti jejího dalšího využití. Věnoval jsem se vysvětlení principu chytrých kontraktů, které se v posledních letech hlavně díky popularitě kryptoměn stále častěji objevují. V posledních dvou pasážích shrnuji hlavní výhody a nevýhody blockchainu. Nakonec jsem se zaměřil na návrh aplikačního řešení v energetickém průmyslu a jeho výslednému vyhodnocení.

Blockchain bude potřeba standardizovat, aby mohla být zajištěna úspěšná implementace ve společnosti. Námořní obchod je mezinárodní záležitostí a pokud se osvědčí použití blockchainu v této části dodavatelského řetězce, myslím si že se snadněji rozšíří do dalších odvětví nejen dodavatelského řetězce.

Od doby, kdy byla poprvé spuštěna Bitcoinová síť, už uplynulo více než deset let a bitcoin způsobil rozruch po celém světě. Nicméně komplex použitých technologií umožnil vznik nové platformy – řetězce bloků, až později se objevilo populární spojení blockchain. Blockchain se ukázal jako průlomová technologie nového tisíciletí, nicméně je potřeba pamatovat na to, že stále existují určitá omezení a potenciální rizika.

Vzhledem k neměnné a transparentní povaze blockchainu je paradoxně problém zabezpečení dat. Zpětná neměnnost omezuje jakoukoliv úpravu dat a transparentnost způsobuje, že data jsou sice chráněna, ale jsou dostupná úplně všem, což ne vždy je žádoucí.

Ještě bude potřeba hodně času, úspěšná testování a experimentování, pro přesvědčení lidí k přechodu na jinou (novou) platformu. Za desítky, možná stovky let si lidé zvykli na zapojení třetích stran do každodenních transakcí. Zavedení digitalizace s sebou nese také obavy ztráty zaměstnání na některých pracovních pozicích.

Seznam zdrojů

[1] *Ledger Academy: Learn Blockchain Basics* [ledger.com] [online]. 2021-01-14 [cit. 2022-03-04]. Dostupné z: https://www.ledger.com/academy/basic-basics/about-crypto/learn-blockchain-basics.

[2] STROUKAL, Dominik. *Před deseti lety vznikl návrh Bitcoinu. Slovo blockchain v něm nenajdete* [Roklen24.cz] [online]. 2018-10-31 [cit. 2022-02-01]. Dostupné z: https://roklen24.cz/pred-deseti-lety-vznikl-navrh-bitcoinu-slovo-blockchain-v-nem-nenajdete/.

[3] Blockchain. In: *Wikipedie* [online]. 2022 [cit. 2022-02-26]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Blockchain&oldid=20979755. Page Version ID: 20979755.

[4] ARCOS, Luis Claudio. The blockchain technology on the music industry. *Brazilian Journal of Operations & Production Management*. 2018, roč. 15, s. 439–443. Dostupné z DOI: 10.14488/BJOPM.2018.v15.n3.a11.

[5] TOURON, Manfred. *Centralized vs Decentralized vs Distributed Systems · Berty Technologies* [berty.tech] [online] [cit. 2022-03-04]. Dostupné z: https://berty.tech/blog/decentralized-distributed-centralized.

[6] SOMMERVILLE, Ian. *Softwarové inženýrství*. Brno: Computer Press, 2013. ISBN 978-80-251-3826-7. OCLC: 862711861.

[7] ZHENG, Zibin; XIE, Shaoan; DAI, Hongning; CHEN, Xiangping; WANG, Huaimin. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In: *2017 IEEE International Congress on Big Data (BigData Congress)*. 2017, s. 557–564. Dostupné z DOI: 10.1109/BigDataCongress.2017.85.

[8] WERGZYN, Kathleen E.; WANG, Eugenia. *Types of Blockchain: Public, Private, or Something in Between | Foley & Lardner LLP* [Foley.com] [online]. 2021-08-19 [cit. 2022-03-04]. Dostupné z: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between.

[9] KALOUSEK, Zbyněk. *Blockchain – o co se jedná a jak funguje (1. díl)* [Kurzy.cz] [online] [cit. 2022-03-03]. Dostupné z: https://www.kurzy.cz/zpravy/609930-blockchain--o-co-se-jedna-a-jak-funguje-1-dil/.

[10] *Block* [binanceacademy.com] [online] [cit. 2022-03-04]. Dostupné z: https://academy.binance.com/en/glossary/block.

[11] BURDA, Karel. *Uvod do kryptografie*. 2015. ISBN 978-80-7204-925-7.

[12] *How does a blockchain transaction work?* [ledger.com] [online]. 2022-01-13 [cit. 2022-03-17]. Dostupné z: https://www.ledger.com/academy/how-does-a-blockchain-transaction-work.

[13] *Blockchain Version - Javatpoint* [javatpoint.com] [online] [cit. 2022-02-06]. Dostupné z: https://www.javatpoint.com/blockchain-version.

[14] DUBEY, Ruchika. *History of Blockchain: A Brief Overview of Three Generations* [blog.knoldus.com] [online]. 2021-09-02 [cit. 2022-02-06]. Dostupné z: http://blog.knoldus.com/history-of-blockchain-a-brief-overview-of-three-generations/.

[15] PETERKA, Jiří. *Báječný svět elektronického podpisu*. Praha: CZ, 2011. ISBN 978-80-904248-3-8. OCLC: 757679149.

[16] MARAM, Balajee. Bitcoin Generation using Blockchain Technology. *JOIV : International Journal on Informatics Visualization*. 2018, roč. 2, s. 127. Dostupné z DOI: 10.30630/joiv.2.3.109.

[17] Asymetrická kryptografie. In: *Wikipedie* [online]. 2021 [cit. 2022-03-04]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Asymetrick%C3%A1_kryptografie&oldid=20731940. Page Version ID: 20731940.

[18] *Consensus mechanisms* [ethereum.org] [online] [cit. 2022-03-04]. Dostupné z: https://ethereum.org.

[19] LEE, David (ed.). *Handbook of blockchain, digital finance, and inclusion*. London, United Kingdom : San Diego, CA: Academic Press, an imprint of Elsevier, 2018. ISBN 978-0-12-810441-5 978-0-12-812282-2. OCLC: on1012492252.

[20] *Proof of Work (PoW) Consensus* [GeeksforGeeks.org] [online]. 2019-01-09 [cit. 2022-03-04]. Dostupné z: https://www.geeksforgeeks.org/proof-of-work-pow-consensus/. Section: Technical Scripter.

[21] MEET, Patel. *Consensus Algorithms in Blockchain* [GeeksforGeeks.org] [online]. 2019-04-25 [cit. 2022-03-15]. Dostupné z: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/. Section: GBlog.

[22] MIKA, František. *Informační logistika* [SystemOnLine.cz] [online]. 2012-03 [cit. 2022-03-22]. Dostupné z: https://www.systemonline.cz/bpm-procesni-rizeni/informacni-logistika.htm. ISSN: 1802-615X.

[23] ANDROULAKI, Elli; BARGER, Artem; BORTNIKOV, Vita; CACHIN, Christian; CHRISTIDIS, Konstantinos; DE CARO, Angelo; ENYEART, David; FERRIS, Christopher; LAVENTMAN, Gennady; MANEVICH, Yacov; MURALIDHARAN, Srinivasan; MURTHY, Chet; NGUYEN, Binh; SETHI, Manish; SINGH, Gari; SMITH, Keith; SORNIOTTI, Alessandro; STATHAKOPOULOU, Chrysoula; VUKOLIĆ, Marko; COCCO, Sharon Weed; YELLICK, Jason. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: *Proceedings of the Thirteenth EuroSys Conference* [online]. Porto Portugal: ACM, 2018, s. 1–15 [cit. 2022-03-23]. ISBN 978-1-4503-5584-1. Dostupné z DOI: 10.1145/3190508.3190538.

[24] BELOVA, Kira. *TradeLens by Maersk - IBM Blockchain Supply Chain Solution* [pixelplex.io] [online]. 2021-02-10 [cit. 2022-03-25]. Dostupné z: https://pixelplex.io/blog/maersk-ibm-tradelens-blockchain-supply-management/.

[25] *Solution Architecture - TradeLens Documentation* [docs.tradelens.com] [online]. 2018 [cit. 2022-03-25]. Dostupné z: https://docs.tradelens.com/learn/solution_architecture/.

[26] INSIGHTS, Ledger. *Canadian Pacific railway joins TradeLens blockchain network* [ledgerinsights.com] [online]. 2020-10-12 [cit. 2022-03-25]. Dostupné z: https://www.ledgerinsights.com/canadian-pacific-railway-joins-tradelens-blockchain-network/.

[27] *ELA Blockchain Services a.s.* [ELA Blockchain Services a.s..cz] [online] [cit. 2022-04-12]. Dostupné z: https://www.elachain.cz.

[28] *Blockchain Notarius* [online] [cit. 2022-04-12]. Dostupné z: https://www.blockchainotarius.cz/.

[29] PROKŠ, Jan; ČERNÝ, Tomáš; HAVLE, Otto; HOLOUBEK, JIří; HÝBNER, František; RŮŽIČKA, Jiří; ŠMÍDOVÁ, Věra. *Studie k využití blockchainových technologií v systémech řízení kvality*. Elektrotechnická asociace - servis s.r.o, 2021.

[30] *Diplomachain - Digitální otisk vzdělání do Blockchain technologie* [Diplomachain.cz] [online] [cit. 2022-03-29]. Dostupné z: https://www.diplomachain.cz/.

[31] *Společnost Enbra jako první v Česku zavádí pro své zaměstnance digitální prohlášení o bezinfekčnosti | Enbra* [enbra.cz] [online] [cit. 2022-03-28]. Dostupné z: https://www.enbra.cz/spolecnost-enbra-jako-prvni-v-cesku-zavadi-pro-sve-zamestnance-digitalni-prohlaseni-o-bezinfekcnosti.

[32] KUDLÁČEK, Patrik. *Smart contracts (Chytré kontrakty) - Co jsou a jak fungují? » Finex.cz* [Finex.cz] [online]. 2019-06-22 [cit. 2022-03-04]. Dostupné z: https://finex.cz/chytre-kontrakty-smart-contracts-co-jsou-a-jak-funguji/.

[33] XU, Yongshun; CHONG, Heap-Yih; CHI, Ming. A Review of Smart Contracts Applications in Various Industries: A Procurement Perspective. *Advances in Civil Engineering* [online]. 2021, vol. 2021, s. 1–25 [cit. 2022-02-17]. ISSN 1687-8094, ISSN 1687-8086. Dostupné z DOI: 10.1155/2021/5530755.

[34] *Smart Contracts work in BlockChain* [ntirawen.com] [online] [cit. 2022-03-04]. Dostupné z: https://www.ntirawen.com/2021/05/smart-contracts-work-in-blockchain.html.

[35] *10 Advantages of Using Smart Contracts* [Medium.com] [online]. 2017-12-27 [cit. 2022-03-04]. Dostupné z: https://medium.com/@ChainTrade/10-advantages-of-using-smart-contracts-bc29c508691a.

[36] *Co je smart contract (chytrý kontrakt) a k čemu slouží?* [Buzzmag.cz] [online]. 2021-08-08 [cit. 2022-03-04]. Dostupné z: https://www.buzzmag.cz/smart-contract/. Section: Kryptoměny a technologie.

Seznam grafických objektů

Seznam zkratek

API Application Programming Interface.

CMA CGM Compagnie Maritime d'Affrètement and Compagnie Générale Maritime.

COSCO China Ocean Shipping Company.

COVID-19 **CO**rona**VI**rus **D**isease 20**19**.

GSBN Global Shipping Business Network.

IBM International Business Machines Corporation.

ISO International Standardization Organization.

OOCL Orient Overseas Container Line.

Oracle SCM Oracle Supply Chain Management.

P2P Peer-to-Peer.

PoC Proof of Capacity.

PoET Proof of Elapsed Time.

PoS Proof of Stake.

PoW Proof of Work.

SHA-2 Secure Hash Algorithm.

SWOT **S**trenghts, **W**eaknesses, **O**pportunities, **T**hreats.

Autor BP	Václav Hroch, DiS.
Název BP	Technologie Blockchain v logistických procesech
Studijní program	Logistika
Rok obhajoby BP	2022
Počet stran	39
Počet příloh	-
Vedoucí BP	prof. Mgr. Roman Jašek, Ph.D., DBA
Anotace	Bakalářská práce je zaměřena na technologie, které dohromady vytváří blockchain. Popisuje vývoj blockchainu, princip fungování a způsoby využití v současné informační logistice. Blockchain je distribuovaná účetní kniha, která uchovává seznam všech transakcí. V rámci této práce je navržen koncept řešení využití technologie blockchain v oblasti průmyslových transakcí.
Klíčová slova	blockchain, distribuovaná účetní kniha, hash, logistika, proces
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	